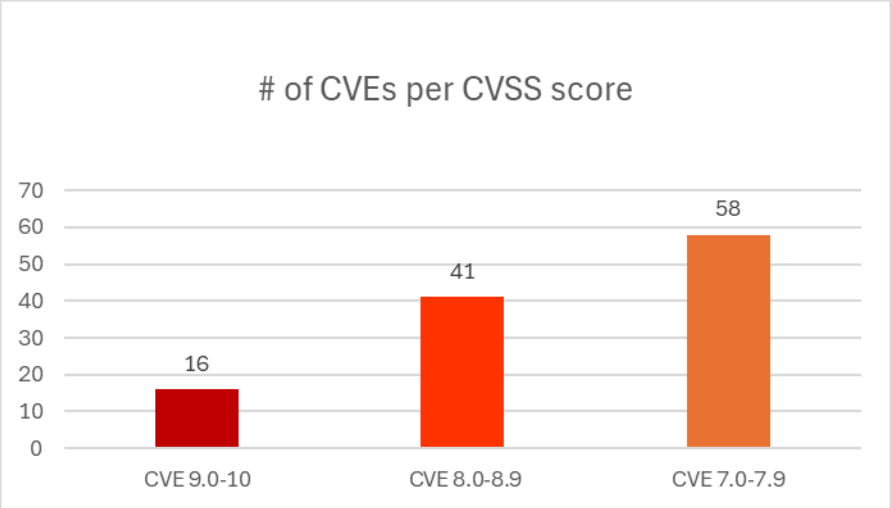
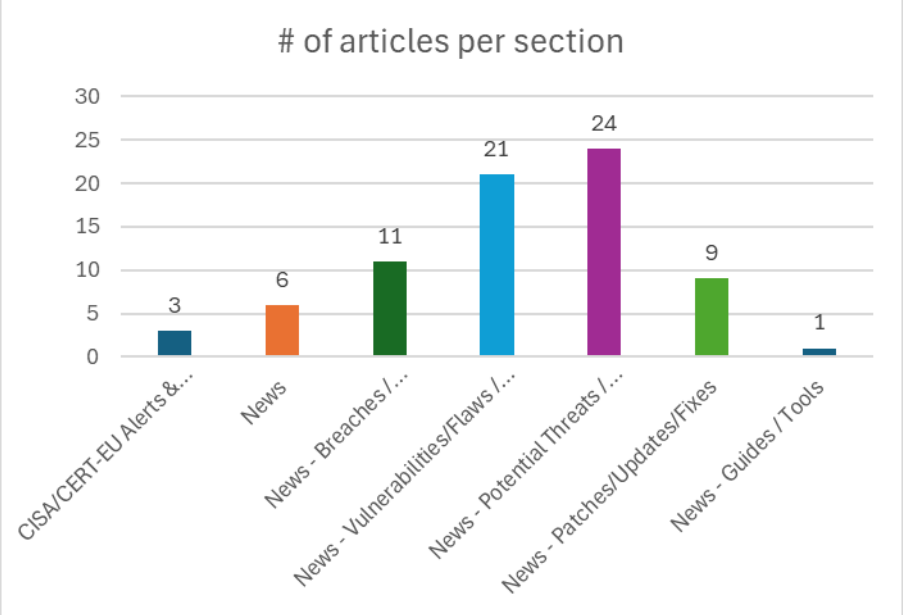


Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 18/11/2026 - 20/11/2026





Contents

Common Vulnerabilities and Exposures (CVEs) 3
CISA/CERT-EU Alerts & Advisories 47
News 48
Breaches / Compromised / Hacked 49
Vulnerabilities / Flaws / Zero-day 50
Patches / Updates / Fixes 51
Potential threats / Threat intelligence 52
Guides / Tools 54
References 55
Annex – Websites with vendor specific vulnerabilities 56

Common Vulnerabilities and Exposures (CVEs)

Η ενότητα αυτή εστιάζει σε ευπάθειες που έχουν καταχωρηθεί πρόσφατα και αξιολογούνται ως σοβαρές, με βάση τη βαθμολογία CVSS. Παρουσιάζονται με σαφήνεια τα συστήματα ή εφαρμογές που επηρεάζονται, ο τύπος όπως ευπάθειας (όπως SQL injection ή command injection) και σχετικοί σύνδεσμοι για περαιτέρω πληροφόρηση ή μέτρα αντιμετώπισης.

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν / Υπηρεσία	Τύπος Ευπάθειας	Περιγραφή (Description)	References
https://nvd.nist.gov/vuln/detail/cve-2026-130778	**10,0**	Incus	Improper Authentication	Incus before 7.6.0 contains an authentication bypass vulnerability that allows remote attackers to authenticate as any trusted certificate by appending its public certificate to their presented TLS client chain. Attackers can append the server's or a cluster member's certificate to gain cluster-level access, bypass authorization, modify trust store entries, and influence scriptlet-based authorization decisions.	https://github.com/lxc/incus/security/advisories/GHSA-xg75-xf37-cph9
https://nvd.nist.gov/vuln/detail/cve-2026-130786	**9,9**	Incus	Improper Neutralization of Special Elements in Output Used by a Downstream Component	Incus before 7.6.0 contains a configuration injection vulnerability that allows users who can launch instances from controlled images to inject LXC directives by embedding line breaks in OCI config.json values or oci.entrypoint and oci.cwd keys. Attackers can add liblxc hooks or crafted tmpfs lxc.mount.entry fields to run commands as root on the host or bind-mount host paths, even from restricted projects.	https://github.com/lxc/incus/security/advisories/GHSA-3wxw-5gh2-j2x2
https://nvd.nist.gov/vuln/detail/cve-2012-20007	**9,8**	ThinkPHP 2.0	Improper Neutralization of Directives in Dynamically Evaluated Code	ThinkPHP 2.0 through 2.2 and 3.0 Lite mode contains an eval injection vulnerability in the Dispatcher PATH_INFO parsing, which uses preg_replace with the /e modifier and a double-quoted replacement. Unauthenticated attackers can send crafted requests to index.php with a malicious 's' parameter containing PHP expressions to execute arbitrary code on the server. Exploitation evidence was first observed by the Shadowserver Foundation on 2023-10-14.	http://web.archive.org/web/20140201221754/http://www.jb51.net:80/softjc/43550.html https://github.com/projectdiscovery/nuclei-templates/blob/main/http/vulnerabilities/thinkphp/thinkphp-2-rce.yaml https://github.com/vulhub/vulhub/tree/master/thinkphp/2-rce https://www.vulncheck.com/advisories/thinkphp-2-x-3.0-lite-unauthenticated-rce-via-dispatcher-path-info

https://nvd.nist.gov/vuln/detail/cve-2026-130675	**9,8**	Craft CMS from 5.0.0	Incorrect Comparison	Craft CMS from 5.0.0 before 5.11.4 contains a remote code execution vulnerability in ImageTransforms::normalizeTransform() that allows attackers to instantiate arbitrary classes by supplying class:null with a __class key. Attackers can reach the method through Craft Commerce's payments/pay redirect template calling customer.photo.getUrl() with a crafted transform to instantiate classes like yii\rbac\PhpManager and execute PHP.	https://github.com/craftcms/cms/security/advisories/GHSA-hq78-cm2m-h24h
https://nvd.nist.gov/vuln/detail/cve-2026-130733	**9,8**	Grav from 2.0.0	Improper Neutralization of Delimiters	Grav from 2.0.0 before 2.2.18 contains an authorization bypass vulnerability that allows publishers to overwrite pages their per-page permissions deny by abusing FolderStorage key delimiter collisions and PageStorage folder reconstruction. Attackers can rename a folder like locked*** or save from a page with an unusual prefix width through a front-end Flex pages form, replacing protected content and permissions to access the protected subtree.	https://github.com/getgrav/grav/security/advisories/GHSA-3rxf-jpgc-hwpv
https://nvd.nist.gov/vuln/detail/cve-2026-130754	**9,8**	LaraDashboard	Improper Authentication	All versions of LaraDashboard contain an authentication bypass in SocialAuthService::findOrCreateUser(), which links a social login to an existing account by email without checking that the OAuth provider verified that email. Unauthenticated attackers using an OAuth/OIDC provider that asserts a victim's email can log in as any user, including Superadmin, and keep persistent access through a linked social_accounts entry.	https://github.com/laradashboard/laradashboard/security/advisories/GHSA-c5x3-wvxj-7cgr
https://nvd.nist.gov/vuln/detail/cve-2026-14492	**9,8**	WordPress Migration Plugin	Unrestricted Upload of File with Dangerous Type	The WP Duplicate – WordPress Migration Plugin plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.1.11 via the save_single_batch_file function. This is due to a PHP type-juggling authentication bypass via loose != comparison with no is_string() guard, combined with unsanitized base64-decoded path construction	https://plugins.trac.wordpress.org/browser/local-sync/tags/1.1.11/admin/class-local-sync-files-op.php#L777 https://plugins.trac.wordpress.org/browser/local-sync/tags/1.1.11/admin/class-local-sync-files-op.php#L800 https://plugins.trac.wordpress.org/browser/local-sync/tags/1.1.11/includes/class-local-sync-handle-server-requests.php#L131 https://plugins.trac.wordpress.org/browser/local-sync/tags/1.1.11/includes/class-local-sync-handle-server-requests.php#L36 https://plugins.trac.wordpress.org/browser/local-sync/tags/1.1.11/includes/class-local-sync-handle-server-requests.php#L400

				in save_single_batch_file() lacking any directory traversal containment. This makes it possible for authenticated attackers, with custom-level access and above, to execute code on the server. Exploitation requires that the site owner has completed the plugin's initial setup so that the site_type and prod_key_random_id options are non-empty, though any non-empty secret value is bypassable via the type-juggling flaw.	https://plugins.trac.wordpress.org/browser/local-sync/tags/1.1.11/includes/class-local-sync.php#L221 https://www.wordfence.com/threat-intel/vulnerabilities/id/26edb085-4737-46a1-be76-b4b955d19aa0?source=cve
https://nvd.nist.gov/vuln/detail/cve-2026-76536	**9,4**	Splunk Enterprise	Improper Authentication	In Splunk Enterprise versions below 10.4.5, 10.2.9, 10.0.12, and 9.4.17, an unauthenticated user could use an empty clustering shared secret to read and modify clustering configuration through the cluster configuration Representational State Transfer (REST) API endpoint on a standalone instance. This could expose clustering configuration, persist attacker-controlled clustering settings, and disrupt clustering operations. The vulnerability is possible because Splunk Enterprise accepts the empty clustering shared secret as a shared-authentication candidate on a standalone instance when clustering is turned off.	https://advisory.splunk.com/advisories/SVD-2026-1103
https://nvd.nist.gov/vuln/detail/cve-2026-115139	**9,3**	Oracle Hyperion Infrastructure	Not specified	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Infrastructure Technology, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as	https://www.oracle.com/security-alerts/cspunov2026.html

				well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N).	
https://nvd.nist.gov/vuln/detail/cve-2026-113425	**9,2**	NGINX	Use After Free	When NGINX Plus or NGINX Open Source is configured as a mail proxy, undisclosed traffic can cause a use-after-free in an nginx worker process. Additionally, attackers can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR. Impact: A remote unauthenticated attacker may crash an nginx worker process or corrupt its memory, disrupting service. Remote code execution is a potential impact. There is no control plane exposure; this is a data plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000163931
https://nvd.nist.gov/vuln/detail/cve-2026-121810	**9,2**	NGINX	Use After Free	This issue affects NGINX Plus and NGINX Open Source configurations that use HTTP/3. A remote, unauthenticated attacker can cause a use-after-free condition in the NGINX worker process, leading to a restart. Exploitation also depends on conditions beyond the attacker's control. Additionally, attackers can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR. Impact: This vulnerability may allow remote attackers to cause a denial-of-service (DoS) on the NGINX system or to possibly trigger a code execution. There is no control plane exposure; this is a data plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000163927
https://nvd.nist.gov/vuln/detail/cve-2026-123007	**9,2**	NGINX	Integer Underflow	This issue affects NGINX Plus or NGINX Open Source configurations that use	https://access.redhat.com/security/cve/cve-2026-123007 https://cyberscoop.com/nginx-critical-vulnerabilities-exploits/

			(Wrap or Wrapa-round)	HTTP/2. When NGINX processes undisclosed traffic, the flow control window can exceed the allowed threshold, potentially resulting in a heap buffer overflow typically followed by an NGINX worker segmentation fault. Additionally, attackers can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR. Impact: An attacker could leverage this vulnerability to crash the NGINX worker process, corrupt its memory, or potentially execute code remotely. There is no control plane exposure; this is a data plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://github.com/Azure/aks-app-routing-operator/issues/623 https://github.com/advisories/GHSA-m4q8-cf44-f42r https://github.com/chainguard-forks/ingress-nginx/pull/69 https://github.com/nginx/nginx/commit/b89c4100bf6762a45e4a6463eaf4b70368277c94 https://github.com/nginx/nginx/issues/2002 https://github.com/openresty/openresty/issues/1165 https://my.f5.com/manage/s/article/K000163926 https://news.ycombinator.com/item?id=50547374 https://nginx.org/en/CHANGES https://nginx2root.com https://ubuntu.com/security/CVE-2026-123007 https://www.rapid7.com/blog/post/ve-cve-2026-123007-critical-nginx-http-2-integer-underflow-leads-to-rce-fixed/ https://www.wiz.io/blog/nginx-http2-rce-vulnerabilities https://xint.io/blog/nginx2root-remote-code-execution
https://nvd.nist.gov/vuln/detail/cve-2026-123633	**9,2**	NGINX	Use After Free	When NGINX Plus or NGINX Open Source is configured to use HTTP/2 for client connections and proxy client requests to a backend, a specially crafted request can result in use-after-free in the worker process, if this process is running low on worker_connections. Additionally, attackers can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR. Impact: This vulnerability may allow remote attackers to cause a denial-of-service (DoS) on the NGINX system or may allow a code execution. There is no control plane exposure; this is a data plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://access.redhat.com/security/cve/cve-2026-123633 https://github.com/Azure/aks-app-routing-operator/issues/623 https://github.com/advisories/GHSA-7xxj-p8w5-434q https://github.com/chainguard-forks/ingress-nginx/pull/68 https://github.com/nginx/nginx/commit/0c87dd1db413e440a4e3ef7ee8acc518509e8809 https://github.com/nginx/nginx/issues/2002 https://github.com/openresty/openresty/issues/1165 https://my.f5.com/manage/s/article/K000163928 https://news.ycombinator.com/item?id=50547374 https://nginx.org/en/CHANGES https://nginx2root.com https://ubuntu.com/security/CVE-2026-123633 https://www.wiz.io/blog/nginx-http2-rce-vulnerabilities https://xint.io/blog/nginx2root-remote-code-execution
https://nvd.nist.gov/vuln/detail/cve-2026-123634	**9,2**	NGINX	Use After Free	This issue occurs when NGINX Plus or NGINX Open Source is configured as a proxy, the proxied server name includes variables, and a Server Side Includes (SSI) or mirror directive sends a subrequest to a location that resolves the same server name. Under these conditions, a specially crafted HTTP request may cause a use-after-free condition in a worker process. An attacker may also be able to execute code if Address Space Layout Randomization	https://my.f5.com/manage/s/article/K000163925

				(ASLR) is disabled or the attacker can bypass ASLR. Impact: An attacker could leverage this vulnerability to crash the NGINX worker process, corrupt its memory, or perform remote code execution (RCE) Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	
https://nvd.nist.gov/vuln/detail/cve-2026-132142	**9,1**	DrayTek Vigor2960	Improper Restriction of Operations within the Bounds of a Memory Buffer; Stack-based Buffer Overflow	A flaw has been found in DrayTek Vigor2960 up to 1.5.1.6. This affects the function dataflowstatus of the file /cgi-bin/mainfunction.cgi of the component CGI Process. This manipulation of the argument option causes stack-based buffer overflow. The attack can be initiated remotely. The exploit has been published and may be used. Upgrading to version 1.5.1.7 is able to mitigate this issue. You should upgrade the affected component. The vendor recommends: "1.5.1.6 isn't the latest version of 2960, the latest version fixes many security issues. And we have another one in our release plan which should solve the issues reported."	https://fw.draytek.com.tw/Vigor2960/Firmware/v1.5.1.7/Vigor2960_v1.5.1.7.zip https://github.com/yikesoftware/DrayTek_Vigor2960_Security_Analysis/tree/main/cases/DRV2960-0024-authenticated-dataflowstatus-option-stack-overflow https://vuldb.com/cve/CVE-2026-132142 https://vuldb.com/submit/1044969 https://vuldb.com/vuln/439442 https://vuldb.com/vuln/439442/cti
https://nvd.nist.gov/vuln/detail/cve-2026-130679	**9,0**	SiYuan	Improper Neutralization of Input During Web Page Generation	SiYuan before 3.8.10 contains a stored cross-site scripting vulnerability in genAVValueHTML() that allows attackers who can store Attribute View asset values to inject script through an unescaped image src attribute. Attackers can store an image URL containing a double quote and onerror handler that executes OS commands via Node.js in the desktop app when victims open the bound note or row attribute panel.	https://github.com/siyuan-note/siyuan/commit/3f4a2ca741411ebf0908ef1b7b86500a4ef4c20c https://github.com/siyuan-note/siyuan/security/advisories/GHSA-3qqh-fmrp-8vfq
https://nvd.nist.gov/vuln/detail/cve-2026-130709	**8,8**	NocoDB	Improper Control of Generation of Code	NocoDB before 2026.09.0 contains a server-side template injection vulnerability that allows authenticated Creator or Owner users to execute JavaScript by abusing Handlebars webhook helpers. Attackers can supply property paths like constructor.constructor to pluck, sortBy, filter, or withSort helpers to reach the Function constructor and run operating-system commands.	https://github.com/nocodb/nocodb/security/advisories/GHSA-72fw-g74f-8mwr

https://nvd.nist.gov/vuln/detail/cve-2026-130741	**8,8**	Grav from 2.0.0	Exposure of Sensitive Information to an Unauthorized Actor	Grav from 2.0.0 before 2.2.18 contains a Twig sandbox bypass vulnerability that allows publishers to read any server file by abusing allowlisted array_key_value() and page accessor setters such as filePath(). Attackers can repoint page objects or overwrite the assets collections to render private keys and the API signing secret, then forge a super-admin API token.	https://github.com/getgrav/grav/security/advisories/GHSA-8rhf-56h6-j77w
https://nvd.nist.gov/vuln/detail/cve-2026-130774	**8,8**	Incus	Improper Privilege Management	Incus before 7.6.0 contains a privilege escalation vulnerability: rebuilding a never-started unprivileged container makes it boot without a user namespace. Root processes inside the container run as host uid 0, keeping capabilities like sys_module, with no device cgroup restriction, letting them load kernel modules and compromise the host.	https://github.com/lxc/incus/security/advisories/GHSA-9c46-v3hw-v6m8
https://nvd.nist.gov/vuln/detail/cve-2026-131236	**8,8**	Splunk Enterprise Security	Improper Neutralization of Special Elements in Data Query Logic	In Splunk Enterprise Security versions below 8.7.0, an unauthenticated user who can influence indexed event data could store attacker-controlled values in event fields. If another authenticated user who reviews the event selects the View Adaptive Response Invocations or View Adaptive Response Results workflow action from Event Actions, Splunk Enterprise Security could run attacker-controlled Search Processing Language (SPL) commands using the permissions of the user who selects the action. The unauthenticated user could then access or modify sensitive data and disrupt services available to the user who selects the action. The vulnerability is possible because the affected Common Information Model workflow actions insert the orig_sid and orig_rid event-field values directly into searches without safely validating or quoting the values. For more information see About workflow actions in Splunk Web (https://help.splunk.com/en/splunk-enterprise/manage-knowledge-objects/knowledge-management-man-	https://advisory.splunk.com/advisories/SVD-2026-1106

				ual/10.2/workflow-actions/about-workflow-actions-in-splunk-web) in the Splunk documentation.	
https://nvd.nist.gov/vuln/detail/cve-2026-131271	**8,8**	Splunk SOAR	Incorrect Authorization	In Splunk SOAR versions below 8.8.0, an authenticated user with permission to view and edit containers for one label could use a slash command through the Representational State Transfer (REST) API to access sensitive product data and credentials outside the authorized container scope. The vulnerability is possible because Splunk SOAR does not enforce authorization for related objects that slash commands access from an authorized artifact.	https://advisory.splunk.com/advisories/SVD-2026-1108
https://nvd.nist.gov/vuln/detail/cve-2026-131851	**8,8**	ILIAS	Improper Neutralization of Special Elements used in an SQL Command	ILIAS before 9.25, 10.13, and 11.6 contains an SQL injection vulnerability in ilPRGAssignmentFilter::toConditions() that allows authenticated users to inject SQL through the StudyProgramme members list Name and Status filters. Attackers holding only the OrgUnit permission to view members can break out of LIKE literals and execute stacked statements, such as overwriting the root password hash to gain administrative control.	https://docu.ilias.de/go/blog/15821/958 https://docu.ilias.de/go/blog/15821/959 https://docu.ilias.de/go/blog/15821/960 https://github.com/ILIAS-eLearning/ILIAS/blob/v11.5/components/ILIAS/StudyProgramme/classes/model/Assignments/ilPRGAssignmentFilter.php#L39-L58 https://github.com/ILIAS-eLearning/ILIAS/blob/v9.24/Modules/StudyProgramme/classes/model/Assignments/ilPRGAssignmentFilter.php#L39-L58 https://github.com/ILIAS-eLearning/ILIAS/commit/cf9d6254c4878a95d85f5f41fe46a3283a6f1820 https://github.com/ILIAS-eLearning/ILIAS/commit/e02e47f02e04207b1576067d5af334b6d5b9c352 https://github.com/ILIAS-eLearning/ILIAS/commit/fc461040f4aa2d542f3b09112d6dfc849e90946d https://www.vulncheck.com/advisories/ilias-before-9.25-10.13-and-11.6-sql-injection-via-studyprogramme-members-filter
https://nvd.nist.gov/vuln/detail/cve-2026-133172	**8,8**	Cozy Cloud cozy-stack 1.6.62	Authorization Bypass Through User-Controlled Key	Cozy Cloud cozy-stack 1.6.62 before 1.6.69 contains an authorization bypass vulnerability in the shared-drive move handler that allows authenticated users to access other instances' files. Attackers owning a shared drive can name another instance's domain and any directory ID as the move source to copy and delete the victim's file tree.	https://github.com/linagora/cozy-stack/blob/1.6.68/web/sharings/move.go#L250-L263 https://github.com/linagora/cozy-stack/commit/983fe4b1218b8a7d83a2734b5ce2fe04227acc0c https://github.com/linagora/cozy-stack/pull/5179 https://github.com/linagora/cozy-stack/releases/tag/1.6.69 https://hackmd.io/@hieund/cozy-stack-shared-drive-move-cross-instance-authz-bypass https://www.vulncheck.com/advisories/cozy-cloud-cozy-stack-1.6.62-before-1.6.69-authorization-bypass-via-shared-drive-move
https://nvd.nist.gov/vuln/detail/cve-2026-133307	**8,8**	Png_Decode in src/Bitmap.c	Out-of-bounds Write	ClassiCube before 1.4.0 contains a heap-based out-of-bounds write vulnerability in Png_Decode in src/Bitmap.c that allows malicious servers to corrupt client memory by sending a PNG with a duplicate IHDR chunk. Attackers can supply	https://github.com/ClassiCube/ClassiCube https://github.com/ClassiCube/ClassiCube/blob/1.3.9/src/Bitmap.c#L529 https://github.com/ClassiCube/ClassiCube/commit/c461fa759f218e3c6bda4642b9af79a98dc84a43 https://github.com/ClassiCube/ClassiCube/releases/tag/1.4.0

				crafted PNGs via texture pack URLs or player skins so the unreset bufferIdx underflows remaining space, letting IDAT data overflow the buffer to crash clients or execute code.	https://www.vulncheck.com/advisories/classicube-before-1.4.0-heap-out-of-bounds-write-via-png-decode-duplicate-ihdr
https://nvd.nist.gov/vuln/detail/cve-2026-115120	**8,7**	Oracle Hyperion Financial	Not specified	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Financial Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N).	https://www.oracle.com/security-alerts/cspunov2026.html
https://nvd.nist.gov/vuln/detail/cve-2026-115164	**8,7**	Oracle Hyperion Infrastructure	Not specified	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows high privileged attacker with network access via T3, IIOP to compromise Oracle Hyperion Infrastructure Technology. While the vulnerability is in Oracle Hyperion Infrastructure Technology, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology	https://www.oracle.com/security-alerts/cspunov2026.html

				accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N).	
https://nvd.nist.gov/vuln/detail/cve-2026-131258	**8,7**	Splunk SOAR	Improper Neutralization of Input During Web Page Generation	In Splunk SOAR versions below 8.8.0, a user with edit permission for a container or workbook task could store attacker-controlled Hypertext Markup Language (HTML) in a note. When another user with view permission for the affected container and its notes opens the affected note in Mission Control, the note could run unauthorized JavaScript code in the browser of that user, expose data available through the authenticated session, and perform actions available through the authenticated session. The vulnerability is possible because Splunk SOAR does not neutralize active content in all notes before Mission Control renders them.	https://advisory.splunk.com/advisories/SVD-2026-1108
https://nvd.nist.gov/vuln/detail/cve-2026-131260	**8,7**	Splunk SOAR	Improper Neutralization of Input During Web Page Generation	In Splunk SOAR versions below 8.8.0, a user with the containers:edit permission could import a container that includes a malicious Hypertext Markup Language (HTML) note. When another user views the imported note, Splunk SOAR could run unauthorized JavaScript in the browser of that user, exposing data and allowing actions available to that user. The vulnerability is possible because Splunk SOAR does not sanitize HTML note content during container import before it renders the content in Mission Control.	https://advisory.splunk.com/advisories/SVD-2026-1108
https://nvd.nist.gov/vuln/detail/cve-2026-127306	**8,6**	Oracle AutoVue	Not specified	Vulnerability in the Oracle AutoVue product of Oracle Supply Chain (component: Security Related Issues). The supported version that is affected is 21.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle AutoVue.	https://www.oracle.com/security-alerts/cspunov2026.html

				While the vulnerability is in Oracle AutoVue, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle AutoVue accessible data. CVSS 3.1 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	
https://nvd.nist.gov/vuln/detail/cve-2026-133528	**8,6**	BeamNG.drive	Out-of-bounds Write	BeamNG.drive before 0.40.6 contains an out-of-bounds write vulnerability because JIT-compiled LuaJIT traces omit FFI array bounds checks, letting untrusted Lua escape the sandbox. Attackers supplying a malicious mod can JIT-compile an FFI store loop, write out of range using a tostring() address leak, re-enable ffi.load, and run commands as the game user.	https://github.com/drbloop2000/BeamNG-Drive-RCE https://store.steampowered.com/news/app/284160/view/681890829846973542 https://www.vulncheck.com/advisories/beamng-drive-before-0.40.6-luajit-ffi-sandbox-escape-via-jit-bounds-check-bypass
https://nvd.nist.gov/vuln/detail/cve-2026-115173	**8,5**	Oracle Hyperion Infrastructure	Not specified	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Security). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. While the vulnerability is in Oracle Hyperion Infrastructure Technology, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N).	https://www.oracle.com/security-alerts/cspunov2026.html
https://nvd.nist.gov/vuln/detail/cve-2026-115179	**8,4**	Oracle Hyperion	Not specified	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Security).	https://www.oracle.com/security-alerts/cspunov2026.html

		Infrastructure		The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Infrastructure Technology executes to compromise Oracle Hyperion Infrastructure Technology. While the vulnerability is in Oracle Hyperion Infrastructure Technology, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 8.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N).	
https://nvd.nist.gov/vuln/detail/cve-2026-130770	**8,4**	Incus	Exposure of Resource to Wrong Sphere	Incus before 7.6.0 creates the NBD servers used for virtual machine migration and disk export on abstract unix sockets, which have no permission checks and whose names are visible in /proc/net/unix. A local unprivileged user can connect while an operation runs to read or modify the VM disk, gaining code execution in the guest on a migration's receiving side.	https://github.com/lxc/incus/security/advisories/GHSA-3rgf-297m-775x
https://nvd.nist.gov/vuln/detail/cve-2018-25442	**8,3**	Baidu UEditor 1.4.0	Server-Side Request Forgery	Baidu UEditor 1.4.0 before 1.4.3.1 contains a server-side request forgery vulnerability that allows unauthenticated attackers to make arbitrary requests via the source[] parameter in /ueditor/jsp/controller.jsp?action=catchimage. Attackers can supply crafted URLs that the ImageHunter component fetches through url.openConnection() to reach internal services and bypass network restrictions. Exploitation evidence was first observed by the Shadowserver Foundation on 2024-07-03.	https://github.com/fex-team/ueditor/blob/v1.4.3/jsp/src/com/baidu/ueditor/hunter/ImageHunter.java https://github.com/projectdiscovery/nuclei-templates/blob/main/http/vulnerabilities/ueditor/ueditor-ssrf.yaml https://www.seebug.org/vuldb/ssvid-97311 https://www.vulncheck.com/advisories/baidu-ueditor-1.4.0-1.4.3.1-ssrf-via-controller-jsp-catchimage https://www.vulncheck.com/advisories/baidu-ueditor-1.4.0-before-1.4.3.1-ssrf-via-controller-jsp-catchimage

https://nvd.nist.gov/vuln/detail/cve-2026-130701	**8,3**	NocoDB	Improper Neutralization of Special Elements used in an SQL Command	NocoDB before 2026.10.1 contains an SQL injection vulnerability because select-field option titles are embedded into MySQL or MariaDB enum/set column definitions with only single-quote doubling, leaving backslashes unescaped. A base creator or owner can end an option title with a backslash to escape the literal and append ALTER TABLE clauses, adding, dropping or renaming columns and altering indexes in the connected database.	https://github.com/nocodb/nocodb/security/advisories/GHSA-fx53-qf4h-cx38
https://nvd.nist.gov/vuln/detail/cve-2026-131203	**8,3**	Splunk Enterprise Security	Incorrect Permission Assignment for Critical Resource	In Splunk Enterprise Security versions below 8.7.0, a user who holds the "ess_analyst" Splunk Enterprise Security role could modify a search macro associated with risk exclusions. Scheduled Risk data model acceleration searches could later run attacker-controlled Search Processing Language (SPL) commands from that macro with elevated permissions. With this access, the user who modified the search macro could expose stored credentials and modify indexes or lookup data available to those searches. The vulnerability is possible because the Splunk Enterprise Security app metadata grants the "ess_analyst" role write access to the risk exclusion search macro. For more information see Users and roles for Splunk Enterprise Security (https://help.splunk.com/en/splunk-enterprise-security-8/install/8.7/installation/users-and-roles-for-splunk-enterprise-security), Finding exclusions in Splunk Enterprise Security (https://help.splunk.com/en/splunk-enterprise-security-8/administer/8.3/user-and-entity-behavior-analytics/finding-exclusions-in-splunk-enterprise-security), and Use search macros in searches (https://help.splunk.com/en/splunk-enterprise/manage-knowledge-objects/knowledge-management-manual/10.4/search-macros/use-search-macros-in-searches) in the Splunk documentation.	https://advisory.splunk.com/advisories/SVD-2026-1106

https://nvd.nist.gov/vuln/detail/cve-2026-131215	**8,3**	Splunk Enterprise Security	Improper Neutralization of Special Elements in Output Used by a Downstream Component	In Splunk Enterprise Security versions below 8.7.0, a user that holds a role with the ueba_finding_exclusion_edit capability could store attacker-controlled values in a User and Entity Behavior Analytics (UEBA) finding exclusion rule. Splunk Enterprise Security could later run attacker-controlled Search Processing Language (SPL) commands from the rule with elevated permissions. With this access, the user could cause Splunk Enterprise Security to read stored credentials and modify lookups and knowledge objects. The vulnerability is possible because the UEBA finding exclusion workflow does not escape user-controlled rule values before using them in generated SPL. For more information see Create a finding exclusion rule using UEBA configuration page (https://help.splunk.com/en/splunk-enterprise-security-8/administer/8.7/user-and-entity-behavior-analytics/finding-exclusions-in-splunk-enterprise-security/create-a-finding-exclusion-rule-using-ueba-configuration-page) and Users and roles for Splunk Enterprise Security (https://help.splunk.com/en/splunk-enterprise-security-8/install/8.7/installation/users-and-roles-for-splunk-enterprise-security) in the Splunk documentation.	https://advisory.splunk.com/advisories/SVD-2026-1106
https://nvd.nist.gov/vuln/detail/cve-2026-131218	**8,3**	Splunk Enterprise Security	Improper Neutralization of Special Elements in Data Query Logic	In Splunk Enterprise Security versions below 8.7.0, a user that holds a role with the mc_investigation_read capability could inject arbitrary Search Processing Language (SPL) into Mission Control dashboard search requests. Mission Control could then run the injected SPL with elevated permissions. With this access, the user could cause Mission Control to read stored credentials and write data to indexes and lookups. The vulnerability is possible because Mission Control does not validate reserved search filters before adding them to dashboard searches. For more information see Overview of Mission Control in Splunk Enterprise Security	https://advisory.splunk.com/advisories/SVD-2026-1106

				(https://help.splunk.com/en/splunk-enterprise-security-8/user-guide/8.1/mission-control/overview-of-mission-control-in-splunk-enterprise-security) and Capability reference for Splunk Enterprise Security (https://help.splunk.com/en/splunk-enterprise-security-8/install/8.2/installation/capability-reference-for-splunk-enterprise-security) in the Splunk documentation.	
https://nvd.nist.gov/vuln/detail/cve-2019-25784	**8,2**	FineCMS	Improper Neutralization of Special Elements used in an SQL Command	FineCMS versions 5.0.4 before 5.0.11 contain an unauthenticated SQL injection vulnerability in the data2 API action handled by list_tag in libraries/Template.php. Attackers can send GET requests to index.php?c=api&m=data2 with a valid auth hash and the param action=sql sql='...' to execute arbitrary SELECT queries and extract database information. Exploitation evidence was first observed by the Shadowserver Foundation on 2023-10-14.	http://www.cnblogs.com/ichunqiu/p/10944669.html https://github.com/projectdiscovery/nuclei-templates/blob/main/http/vulnerabilities/other/finecms-sqli.yaml https://www.vulncheck.com/advisories/finecms-5.0.4-5.0.11-sql-injection-via-api-data2-param https://www.vulncheck.com/advisories/finecms-5.0.4-before-5.0.11-sql-injection-via-api-data2-param
https://nvd.nist.gov/vuln/detail/cve-2021-48021	**8,2**	Chamilo LMS 1.11.10	Improper Neutralization of Special Elements used in an SQL Command	Chamilo LMS 1.11.10 before 1.11.16 contains an unauthenticated SQL injection vulnerability in the searchOptionsFromTags function through the options parameter of extra_field.ajax.php. Attackers can send POST requests with a malicious JSON options array to inject SQL into the IN clause and extract database information. Exploitation evidence was first observed by the Shadowserver Foundation on 2023-10-14.	https://github.com/chamilo/chamilo-lms/commit/23787842c2013db318e82d6987469fc8b17df0f8 https://github.com/chamilo/chamilo-lms/commit/e8332fd9d5607ae7866e27936b4376ea1053ae03 https://github.com/projectdiscovery/nuclei-templates/blob/main/http/vulnerabilities/other/chamilo-lms-sqli.yaml https://www.vulncheck.com/advisories/chamilo-lms-1.11.10-1.11.16-sql-injection-via-extra-field-ajax-php https://www.vulncheck.com/advisories/chamilo-lms-1.11.10-before-1.11.16-sql-injection-via-extra-field-ajax-php
https://nvd.nist.gov/vuln/detail/cve-2022-51028	**8,2**	CmsEasy 7.7.5_20210919	Improper Neutralization of Special Elements used in an SQL Command	CmsEasy 7.7.5_20210919 contains an unauthenticated SQL injection vulnerability in the execsql_action function at /?case=crossall&act=execsql that executes attacker-supplied queries decrypted with the hardcoded key 'cmseasy_sql'. Attackers can send a crafted 'sql' parameter to run arbitrary SQL and dump the admin username and password hash. Exploitation evidence was first observed by the Shadowserver Foundation on 2023-10-22.	https://cn-sec.com/archives/1580677.html https://github.com/PeiQi0/PeiQi-WIKI-Book/blob/main/docs/wiki/cms/CmsEasy/CmsEasy%20crossall_act.php%20SQL%E6%B3%A8%E5%85%A5%E6%BC%8F%E6%B4%9E.md https://github.com/projectdiscovery/nuclei-templates/blob/main/http/vulnerabilities/other/cmseasy-crossall-act-sqli.yaml https://www.vulncheck.com/advisories/cmseasy-7.7-5-20210919-unauthenticated-sql-injection-via-crossall-execsql
https://nvd.nist.gov/vuln/detail/cve-2024-58402	**8,2**	Azon Dominator releases	Improper Neutraliza-	Azon Dominator releases through 2024-06-03 contain an SQL injection vulnerability that allows unauthenticated attackers	https://github.com/projectdiscovery/nuclei-templates/blob/main/http/vulnerabilities/other/azon-dominator-sqli.yaml https://packetstorm.news/files/id/179283/

			tion of Special Elements used in an SQL Command	to manipulate database queries through the cid parameter in /fetch_products.php. Attackers can send crafted POST requests with boolean-based or time-based blind payloads to extract sensitive database information. Exploitation evidence was first observed by the Shadowserver Foundation on 2024-07-30.	https://www.codester.com/items/12775/azon-dominator-affiliate-marketing-script https://www.exploit-db.com/exploits/52059 https://www.vulncheck.com/advisories/azon-dominator-sql-injection-via-fetch-products-php-cid-parameter
https://nvd.nist.gov/vuln/detail/cve-2026-115082	**8,2**	Oracle Hyperion Infrastructure	Not specified	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Infrastructure Technology, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	https://www.oracle.com/security-alerts/cspunov2026.html
https://nvd.nist.gov/vuln/detail/cve-2026-130683	**8,2**	SiYuan	Improper Limitation of a Pathname to a Restricted Directory	SiYuan before 3.8.10 uses an incomplete deny-list in IsSensitivePath that omits shell-initialization files such as .zshenv and .bash_profile, as well as ~/.local. Authenticated administrators can call /api/file/copyFile with an absolute destination outside the workspace to write payloads there, which execute as the user on the next shell or login.	https://github.com/siyuan-note/siyuan/security/advisories/GHSA-4xfj-946m-258h

https://nvd.nist.gov/vuln/detail/cve-2026-114938	**8,1**	Oracle	Heap-based Buffer Overflow	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle Java SE: 8u511b33-perf, 17.0.21.0.3, 21.0.13.0.3, 25.0.5.0.3, 27.0.1.0.3; Oracle GraalVM for JDK: 17.0.21.0.3 and 21.0.13.0.3; Oracle GraalVM Enterprise Edition: 21.3.20.0.3. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service.	http://www.openwall.com/lists/oss-security/2026/11/17/31 http://www.openwall.com/lists/oss-security/2026/11/19/5 https://access.redhat.com/security/cve/cve-2026-114938 https://calif.io/java4shell https://cert-portal.siemens.com/productcert/html/ssa-272816.html https://cert-portal.siemens.com/productcert/html/ssa-810379.html https://github.com/Azure/azure-functions-java-worker/issues/909 https://github.com/chainguard-dev/cg-skills/pull/17 https://github.com/corretto/corretto-27/blob/27.0.1.1.4/CHANGELOG.md https://news.ycombinator.com/item?id=50538240 https://shiro.apache.org/blog/2026/11/apache-shiro-java4shell.html https://ubuntu.com/security/CVE-2026-114938 https://www.cisa.gov/news-events/alerts/2026/11/17/critical-java-vulnerability-requires-immediate-patching https://www.oracle.com/security-alerts/cspunov2026.html
https://nvd.nist.gov/vuln/detail/cve-2026-115046	**8,1**	Oracle Hyperion Infrastructure	Not specified	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	https://www.oracle.com/security-alerts/cspunov2026.html
https://nvd.nist.gov/vuln/detail/cve-2026-115059	**8,1**	Oracle Hyperion	Not specified	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle	https://www.oracle.com/security-alerts/cspunov2026.html

		Infrastructure		Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 8.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H).	
https://nvd.nist.gov/vuln/detail/cve-2026-115062	**8,1**	Oracle Hyperion Financial	Not specified	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via SOAP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	https://www.oracle.com/security-alerts/cspunov2026.html
https://nvd.nist.gov/vuln/detail/cve-2026-115130	**8,1**	Oracle Hyperion Planning	Not specified	Vulnerability in the Oracle Hyperion Planning product of Oracle Hyperion (component: Application Development Framework). The supported version that is affected is 11.2.26.0.000. Easily exploitable	https://www.oracle.com/security-alerts/cspunov2026.html

				vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Planning. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Planning accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Planning accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	
https://nvd.nist.gov/vuln/detail/cve-2026-115153	**8,1**	Oracle Hyperion Infrastructure	Not specified	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Security). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N).	https://www.oracle.com/security-alerts/cspunov2026.html
https://nvd.nist.gov/vuln/detail/cve-2026-115172	**8,1**	Oracle Hyperion Infrastructure	Not specified	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Security). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized creation,	https://www.oracle.com/security-alerts/cspunov2026.html

				deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	
https://nvd.nist.gov/vuln/detail/cve-2026-127308	**8,1**	Oracle AutoVue	Not specified	Vulnerability in the Oracle AutoVue product of Oracle Supply Chain (component: Security). The supported version that is affected is 21.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle AutoVue. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle AutoVue accessible data as well as unauthorized access to critical data or complete access to all Oracle AutoVue accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N).	https://www.oracle.com/security-alerts/cspunov2026.html
https://nvd.nist.gov/vuln/detail/cve-2026-130721	**8,1**	NocoDB from 2026.06.2	Incorrect Authorization	NocoDB from 2026.06.2 before 2026.08.0 contains an authorization bypass vulnerability that allows authenticated base Editors to write to data-read-only sources by abusing the internal batch endpoint. Attackers can name a writable decoy table on the batch envelope and target a read-only source table in dataUpdate, dataInsert or dataDelete sub-operations to modify or destroy records.	https://github.com/nocodb/nocodb/security/advisories/GHSA-q742-6g25-cvm9
https://nvd.nist.gov/vuln/detail/cve-2026-131200	**8,1**	Splunk Enterprise Security	Incorrect Authorization	In Splunk Enterprise Security versions below 8.7.0, a user who holds the "ess_analyst" Splunk Enterprise Security role could create an attacker-controlled saved	https://advisory.splunk.com/advisories/SVD-2026-1106

				search. Threat intelligence lookup generation could later run the saved search with elevated permissions, which could let the user who created the saved search run arbitrary Search Processing Language (SPL) commands with those permissions. The vulnerability is possible because Splunk Enterprise Security does not restrict threat intelligence lookup generation to the intended saved searches. For more information see Users and roles for Splunk Enterprise Security (https://help.splunk.com/en/splunk-enterprise-security-8/install/8.7/installation/users-and-roles-for-splunk-enterprise-security) and Turn on threat matching searches in Splunk Enterprise Security (https://help.splunk.com/en/splunk-enterprise-security-8/administer/8.0/threat-intelligence/turn-on-threat-matching-searches-in-splunk-enterprise-security) in the Splunk documentation.	
https://nvd.nist.gov/vuln/detail/cve-2026-131210	**8,1**	Splunk Enterprise Security	Improper Input Validation	In Splunk Enterprise Security versions below 8.7.0, a user that holds a role with the ueba_finding_exclusion_edit capability could create a finding exclusion rule that references an attacker-controlled lookup definition if the role also grants write access to globally shared lookup definitions, as the "ess_analyst" Splunk Enterprise Security role does. The User and Entity Behavior Analytics (UEBA) Content App could later include the lookup name in a search and run arbitrary Search Processing Language (SPL) commands with elevated permissions. With this access, the user who created the finding exclusion rule could expose stored credentials and other data outside the permissions assigned to the "ess_analyst" role. The vulnerability is possible because UEBA finding exclusion processing does not safely quote lookup names before including them in SPL searches. For more information see Finding exclusions in Splunk Enterprise Security (https://help.splunk.com/en/splunk-	https://advisory.splunk.com/advisories/SVD-2026-1106

				enterprise-security-8/administer/8.3/user-and-entity-behavior-analytics/finding-exclusions-in-splunk-enterprise-security) and Roles and knowledge objects in UEBA for Splunk Enterprise Security (https://help.splunk.com/en/splunk-enterprise-security-8/administer/8.8/user-and-entity-behavior-analytics/ueba-content-app-for-on-premises/roles-and-knowledge-objects-in-ueba-for-splunk-enterprise-security) in the Splunk documentation.	
https://nvd.nist.gov/vuln/detail/cve-2026-84273	**8,1**	IBM Guardium Data Protection 12.2	Improper Limitation of a Pathname to a Restricted Directory	IBM Guardium Data Protection 12.2 is vulnerable to path traversal in the datasource functionality. An authenticated attacker could exploit this vulnerability to delete arbitrary files on the appliance.	https://www.ibm.com/support/pages/node/7297484
https://nvd.nist.gov/vuln/detail/cve-2026-130766	**8,0**	Obot from 0.26.0	Origin Validation Error	Obot from 0.26.0 before 0.27.0 fails to validate the resource identifier in remote MCP server protected resource metadata, allowing malicious MCP servers to steal access tokens. Attackers can name a different service and authorization server with chosen scopes, causing Obot to obtain the victim's token for that service and forward it to the attacker.	https://github.com/obot-platform/obot/security/advisories/GHSA-x3hf-v55x-jcp6
https://nvd.nist.gov/vuln/detail/cve-2026-127337	**7,9**	Oracle AutoVue	Not specified	Vulnerability in the Oracle AutoVue product of Oracle Supply Chain (component: Security). The supported version that is affected is 21.1.0. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle AutoVue executes to compromise Oracle AutoVue. While the vulnerability is in Oracle AutoVue, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle AutoVue accessible data as well as unauthorized update, insert or delete access to some of Oracle AutoVue accessible data. CVSS 3.1 Base Score 7.9 (Confidentiality and Integrity impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cspunov2026.html

				(CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N).	
https://nvd.nist.gov/vuln/detail/cve-2026-133168	**7,8**	OFFIS DCMTK 3.7.1	Out-of-bounds Write	OFFIS DCMTK 3.7.1 contains a heap buffer overflow vulnerability in togglePlanarConfiguration8 and togglePlanarConfiguration16 in djcodece.cc, which compute row offsets using rows instead of columns. Attackers can supply a crafted color-by-plane DICOM image with more rows than columns that is compressed with the true-lossless JPEG codec to corrupt heap memory, causing crashes and potentially code execution.	https://github.com/DCMTK/dcmtk https://github.com/DCMTK/dcmtk/blob/DCMTK-3.7.1/dcmjpeg/libsrc/djcodece.cc#L1503-L1540 https://github.com/DCMTK/dcmtk/commit/c22836c449bb81834fee5d883e9ebd9d7dab90b9 https://support.dcmtk.org/redmine/issues/1298 https://www.vulncheck.com/advisories/dcmtk-3.7.1-heap-buffer-overflow-via-jpeg-encoder-planar-configuration-conversion
https://nvd.nist.gov/vuln/detail/cve-2026-115129	**7,7**	Oracle Hyperion Planning	Not specified	Vulnerability in the Oracle Hyperion Planning product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Planning. While the vulnerability is in Oracle Hyperion Planning, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Planning accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	https://www.oracle.com/security-alerts/cspunov2026.html
https://nvd.nist.gov/vuln/detail/cve-2026-115158	**7,7**	Oracle Hyperion Infrastructure	Not specified	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. While the vulnerability is in Oracle Hyperion Infrastructure Technology, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access	https://www.oracle.com/security-alerts/cspunov2026.html

				to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	
https://nvd.nist.gov/vuln/detail/cve-2026-115170	**7,7**	Oracle Hyperion Infrastructure	Not specified	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Security). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. While the vulnerability is in Oracle Hyperion Infrastructure Technology, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	https://www.oracle.com/security-alerts/cspunov2026.html
https://nvd.nist.gov/vuln/detail/cve-2026-127349	**7,7**	Oracle Hyperion Financial	Not specified	Vulnerability in the Oracle Hyperion Financial Close Management product of Oracle Hyperion (component: Reconciliation Manage). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Close Management. While the vulnerability is in Oracle Hyperion Financial Close Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Close Management accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	https://www.oracle.com/security-alerts/cspunov2026.html

https://nvd.nist.gov/vuln/detail/cve-2026-130782	**7,7**	Incus	Incorrect Authorization	Incus before 7.6.0 contains an improper authorization vulnerability that allows restricted and view-only clients to read default project resources by requesting the default project directly. Attackers knowing resource names can read profiles, images, network zone peer keys and stored credentials, and export custom volume or bucket backups to obtain full contents or S3 admin keys.	https://github.com/lxc/incus/security/advisories/GHSA-8r3h-vc36-6xpx
https://nvd.nist.gov/vuln/detail/cve-2026-131266	**7,7**	Splunk SOAR	Insertion of Sensitive Information Into Sent Data	In Splunk SOAR versions below 8.8.0, a user that holds a role with the System Settings edit permission could cause Splunk SOAR to send a stored Elasticsearch password to a host that the user controls. The vulnerability is possible because Splunk SOAR reuses a stored Elasticsearch password for a changed Search Settings endpoint without requiring a replacement password.	https://advisory.splunk.com/advisories/SVD-2026-1108
https://nvd.nist.gov/vuln/detail/cve-2026-115058	**7,6**	Oracle Hyperion Infrastructure	Not specified	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Security). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Infrastructure Technology, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).	https://www.oracle.com/security-alerts/cspunov2026.html

https://nvd.nist.gov/vuln/detail/cve-2026-115117	**7,6**	Oracle Hyperion Financial	Not specified	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Management accessible data as well as unauthorized read access to a subset of Oracle Hyperion Financial Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L).	https://www.oracle.com/security-alerts/cspunov2026.html
https://nvd.nist.gov/vuln/detail/cve-2026-115143	**7,6**	Oracle Hyperion Infrastructure	Not specified	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Infrastructure Technology, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cspunov2026.html

				(CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).	
https://nvd.nist.gov/vuln/detail/cve-2026-115176	**7,6**	Oracle Hyperion Infrastructure	Not specified	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Infrastructure Technology, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).	https://www.oracle.com/security-alerts/cspunov2026.html
https://nvd.nist.gov/vuln/detail/cve-2026-127340	**7,6**	Oracle Hyperion Financial	Not specified	Vulnerability in the Oracle Hyperion Financial Close Management product of Oracle Hyperion (component: Reconciliation Manage). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Close Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Financial Close Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Close Management	https://www.oracle.com/security-alerts/cspunov2026.html

				accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Financial Close Management accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).	
https://nvd.nist.gov/vuln/detail/cve-2026-131243	**7,6**	Splunk SOAR	Exposure of Sensitive Information to an Unauthorized Actor	In Splunk SOAR versions below 8.8.0, an authenticated user with permission to view an affected container could query the Representational State Transfer (REST) API for approvals to retrieve a live external prompt link belonging to another user. Using this link, the user could read the approval prompt without authentication and submit a response, potentially disrupting or altering the automated workflow governed by that approval. The vulnerability is possible because the REST API for approvals exposes the live external prompt link without verifying that the requester owns the approval.	https://advisory.splunk.com/advisories/SVD-2026-1108
https://nvd.nist.gov/vuln/detail/cve-2023-54420	**7,5**	LiveBOS builds	Improper Limitation of a Pathname to a Restricted Directory	LiveBOS builds through 2023-08-16 contain a path traversal vulnerability that allows unauthenticated attackers to read arbitrary files via the imgName parameter in /feed/ShowImage.do using a ';.js.jsp' suffix bypass. Attackers can send crafted GET requests with directory traversal sequences in imgName to read system files such as /etc/passwd. Exploitation evidence was first observed by the Shadowserver Foundation on 2023-10-30.	https://github.com/luck-ying/Library-POC/blob/master/2023HW/20238.16/LiveBOS_how-Image.do%E4%BB%BB%E6%84%8F%E6%96%87%E4%BB%B6%E8%AF%BB%E5%8F%96%E6%BC%8F%E6%B4%9E.py https://github.com/projectdiscovery/nuclei-templates/blob/main/http/vulnerabilities/other/livebos-file-read.yaml https://www.vulncheck.com/advisories/livebos-unauthenticated-path-traversal-file-read-via-showimage-do
https://nvd.nist.gov/vuln/detail/cve-2026-115146	**7,5**	Oracle Hyperion Infrastructure	Not specified	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in un-	https://www.oracle.com/security-alerts/cspunov2026.html

				authorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	
https://nvd.nist.gov/vuln/detail/cve-2026-127351	**7,5**	Oracle Hyperion Financial	Not specified	Vulnerability in the Oracle Hyperion Financial Close Management product of Oracle Hyperion (component: Reconciliation Manage). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Close Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Close Management accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	https://www.oracle.com/security-alerts/cspunov2026.html
https://nvd.nist.gov/vuln/detail/cve-2026-130729	**7,5**	NocoDB	Authorization Bypass Through User-Controlled Key	NocoDB before 2026.08.0 contains an authorization bypass in its public shared-view relation endpoints, which verify that a parent record exists but not that it passes the view's row filters. Unauthenticated attackers holding a public share link can supply guessable auto-incrementing ids of filtered-out records to has-many, many-to-many, one-many, or link endpoints to read their child records.	https://github.com/nocodb/nocodb/security/advisories/GHSA-267g-6rgg-2qf9
https://nvd.nist.gov/vuln/detail/cve-2026-130749	**7,5**	Grav from 2.0.0	Allocation of Resources Without Limits or Throttling	Grav from 2.0.0 before 2.2.18 contains a resource exhaustion vulnerability that allows unauthenticated attackers to fill the disk by varying the HTTP Host header. Attackers can send requests with distinct Host values to create per-host compiled configuration, blueprint, language and page index caches, causing session, upload and logging failures.	https://github.com/getgrav/grav/security/advisories/GHSA-j9j4-qq25-7m54

https://nvd.nist.gov/vuln/detail/cve-2026-131190	**7,5**	Splunk Enterprise	Use of Hard-coded Credentials	In Splunk Enterprise versions below 10.4.5, 10.2.9, 10.0.12, and 9.4.17, an unauthenticated user could access RapidDiag process metadata and log file inventory information through the Representational State Transfer (REST) API. The vulnerability is possible because certain RapidDiag REST API endpoints accept a factory-default shared key for node authentication, which lets requests bypass Splunk user authentication. For more information see Using RapidDiag (https://help.splunk.com/en/splunk-enterprise/administer/troubleshoot/9.0/contact-splunk-support/using-rapiddiag) and Secure Splunk Enterprise services with pass4SymmKey (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.0/secure-distributed-and-clustered-splunk-environments/secure-splunk-enterprise-services-with-pass4symmkey) in the Splunk documentation.	https://advisory.splunk.com/advisories/SVD-2026-1103
https://nvd.nist.gov/vuln/detail/cve-2026-131192	**7,5**	Splunk Enterprise	Authentication Bypass by Primary Weakness	In Splunk Enterprise versions below 10.6.1, 10.4.5, 10.2.9, 10.0.12, and 9.4.17, an unauthenticated user could access live event data from the indexing pipeline through the Representational State Transfer (REST) API on a standalone instance or a search head that is not an indexer cluster member. The vulnerability is possible because Splunk Enterprise accepts an empty shared key during service authentication.	https://advisory.splunk.com/advisories/SVD-2026-1103
https://nvd.nist.gov/vuln/detail/cve-2026-131196	**7,5**	Splunk Enterprise	NULL Pointer Dereference	In Splunk Enterprise versions below 10.4.5, 10.2.9, 10.0.12, and 9.4.17, an unauthenticated user who can connect to a Splunk-to-Splunk (S2S) data forwarding receiver could cause the Splunk daemon to terminate unexpectedly. The unexpected termination interrupts data indexing and access to the management API and Splunk Web until the Splunk Enterprise process restarts. The vulnerability is possible because the S2S data forwarding receiver	https://advisory.splunk.com/advisories/SVD-2026-1103

				does not validate an optional field in forwarded event data, which results in a null pointer dereference when the field is missing. For more information see Intermediate data routing using universal and heavy forwarders (https://help.splunk.com/en/splunk-enterprise/get-started/splunk-validated-architectures/getting-data-in-forwarding-and-preprocessing/intermediate-data-routing-using-universal-and-heavy-forwarders) in the Splunk documentation.	
https://nvd.nist.gov/vuln/detail/cve-2026-133534	**7,5**	PowerLink	Improper Neutralization of Special Elements used in an SQL Command	PowerLink developed by Neotroni Lighting has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read database contents.	https://www.twcert.org.tw/en/cp-139-11424-ecbad-2.html https://www.twcert.org.tw/tw/cp-132-11423-cb8d4-1.html
https://nvd.nist.gov/vuln/detail/cve-2026-76414	**7,5**	Microsoft Compiled HTML	Loop with Unreachable Exit Condition	A vulnerability in Microsoft Compiled HTML Help (CHM) file scanning of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to a logic error when scanning the CHM file and following the internal file pointers. An attacker could exploit this vulnerability by sending a crafted CHM file for scanning. A successful exploit could allow the attacker to cause the ClamAV decode process to terminate due to an infinite loop, resulting in a DoS condition on the affected software.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-multi-e93M3vdA
https://nvd.nist.gov/vuln/detail/cve-2026-76416	**7,5**	InstallShield file parser of ClamAV	Loop with Unreachable Exit Condition	A vulnerability in the InstallShield file parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to incomplete error checking when the InstallShield File Parser is performing a scan. An attacker could exploit this vulnerability by sending a crafted InstallShield file to be scanned. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-multi-e93M3vdA

				cause the ClamAV scanning process to terminate due to an infinite loop, resulting in a DoS condition on the affected software.	
https://nvd.nist.gov/vuln/detail/cve-2026-76417	**7,5**	Microsoft Compound File	Uncontrolled Resource Consumption	A vulnerability in Object Linking and Embedding, 2nd Generation (OLE2) file parser for ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to logic error when parsing specifically formatted files with the OLE2 file parser. An attacker could exploit this vulnerability by by sending a crafted Microsoft Compound File Binary (CFB) file to be scanned. A successful exploit could allow the attacker to allocate all available memory, causing the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-multi-e93M3vdA
https://nvd.nist.gov/vuln/detail/cve-2026-76421	**7,5**	Microsoft Compiled HTML	Heap-based Buffer Overflow	A vulnerability in the LZX data algorithm for Microsoft Compiled HTML Help (CHM) file scanning in ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to improper boundary checks when applying the LZX data algorithm to CHM files during the decoder stage, which may result in buffer overflow. An attacker could exploit this vulnerability by sending a crafted CHM file for scanning. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-multi-e93M3vdA
https://nvd.nist.gov/vuln/detail/cve-2026-76515	**7,5**	Microsoft Compound File	Uncontrolled Resource Consumption	A vulnerability in the Object Linking and Embedding, 2nd Generation (OLE2) file parser for ClamAV could allow an unauthenticated, remote attacker to exceed the configured MaxScanTime and cause a DoS condition on an affected device. This vulnerability is due to inefficiencies when parsing specifically formatted files with the OLE2 file parser. An attacker could exploit this vulnerability by by sending a crafted Microsoft Compound File Binary (CFB) file to be scanned. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-multi-e93M3vdA

				exploit could allow the attacker to effectively cause the ClamAV OLE2 parser to get into an infinite loop, resulting in a DoS condition on the affected software.	
https://nvd.nist.gov/vuln/detail/cve-2026-115053	**7,4**	Oracle Hyperion Infrastructure	Not specified	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.26.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	https://www.oracle.com/security-alerts/cspunov2026.html
https://nvd.nist.gov/vuln/detail/cve-2026-115124	**7,4**	Oracle Hyperion Planning	Not specified	Vulnerability in the Oracle Hyperion Planning product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.26.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Hyperion Planning. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Planning accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Planning accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	https://www.oracle.com/security-alerts/cspunov2026.html

https://nvd.nist.gov/vuln/detail/cve-2026-115138	**7,4**	Oracle Hyperion Planning	Not specified	Vulnerability in the Oracle Hyperion Planning product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.26.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Planning. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Planning accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Planning accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	https://www.oracle.com/security-alerts/cspunov2026.html
https://nvd.nist.gov/vuln/detail/cve-2026-115140	**7,4**	Oracle Hyperion Planning	Not specified	Vulnerability in the Oracle Hyperion Planning product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.26.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Hyperion Planning. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Planning accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Planning accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	https://www.oracle.com/security-alerts/cspunov2026.html
https://nvd.nist.gov/vuln/detail/cve-2026-115141	**7,4**	Oracle Hyperion Planning	Not specified	Vulnerability in the Oracle Hyperion Planning product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.26.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Oracle Hyperion Planning. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical	https://www.oracle.com/security-alerts/cspunov2026.html

				data or all Oracle Hyperion Planning accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Planning accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	
https://nvd.nist.gov/vuln/detail/cve-2026-115160	**7,4**	Oracle Hyperion Infrastructure	Not specified	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Security). The supported version that is affected is 11.2.26.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	https://www.oracle.com/security-alerts/cspunov2026.html
https://nvd.nist.gov/vuln/detail/cve-2026-115163	**7,4**	Oracle Hyperion Infrastructure	Not specified	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Security). The supported version that is affected is 11.2.26.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cspunov2026.html

				(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	
https://nvd.nist.gov/vuln/detail/cve-2026-115178	**7,4**	Oracle Hyperion Infrastructure	Not specified	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.26.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	https://www.oracle.com/security-alerts/cspunov2026.html
https://nvd.nist.gov/vuln/detail/cve-2026-127360	**7,4**	Oracle Hyperion Financial	Not specified	Vulnerability in the Oracle Hyperion Financial Close Management product of Oracle Hyperion (component: Reconciliation Manage). The supported version that is affected is 11.2.26.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via SMB to compromise Oracle Hyperion Financial Close Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Close Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Financial Close Management accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	https://www.oracle.com/security-alerts/cspunov2026.html

https://nvd.nist.gov/vuln/detail/cve-2026-131211	**7,3**	Splunk App	Improper Neutralization of Special Elements in Data Query Logic	In Splunk App for Payment Card Industry Compliance versions below 8.7.0, a user who holds the "ess_user" Splunk Enterprise Security role could add attacker-controlled values to lookup data used by the Primary Functions report. If another authenticated user later selects the value in the Primary Function Summary panel, the Splunk App for Payment Card Industry Compliance could run attacker-controlled Search Processing Language (SPL) commands using the permissions of the user who selected the value. With this access, the first user could expose or modify data available to the user who selected the value. The vulnerability is possible because the Primary Functions report does not safely escape report values before including them in drilldown searches. For more information see Users and roles for Splunk Enterprise Security (https://help.splunk.com/en/splunk-enterprise-security-8/install/8.7/installation/users-and-roles-for-splunk-enterprise-security) and Reports (https://help.splunk.com/en/splunk-enterprise-security-8/splunk-app-for-pci-compliance/user-manual/8.7/using-the-splunk-app-for-pci-compliance/reports) in the Splunk documentation.	https://advisory.splunk.com/advisories/SVD-2026-1106
https://nvd.nist.gov/vuln/detail/cve-2026-132611	**7,3**	SourceCodester	Improper Access Control; Unrestricted Upload of File with Dangerous Type	A security vulnerability has been detected in SourceCodester Simple Form Builder Web App 1.0. This impacts the function save_response of the file /classes/Forms.php. The manipulation of the argument q[<index>] leads to unrestricted upload. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	https://github.com/wsx138/cve/issues/10 https://vuldb.com/cve/CVE-2026-132611 https://vuldb.com/submit/1045192 https://vuldb.com/vuln/439746 https://vuldb.com/vuln/439746/cti https://www.sourcecodester.com/
https://nvd.nist.gov/vuln/detail/cve-2026-132626	**7,3**	SourceCodester	Improper Neutralization of Special Elements in Output Used by a	A vulnerability was identified in SourceCodester Modern Ticket Reservation System 1.0. Affected by this vulnerability is an unknown functionality of the file /booking/validate.php. The manipulation of the argument ticket leads to sql injection. It is possible to initiate the attack remotely.	https://github.com/wsx138/cve/issues/12 https://vuldb.com/cve/CVE-2026-132626 https://vuldb.com/submit/1045348 https://vuldb.com/vuln/439770 https://vuldb.com/vuln/439770/cti https://www.sourcecodester.com/

			Downstream Component; Improper Neutralization of Special Elements used in an SQL Command	The exploit is publicly available and might be used.	
https://nvd.nist.gov/vuln/detail/cve-2026-116758	**7,2**	The Advanced Country Blocker plugin for WordPress	Improper Neutralization of Input During Web Page Generation	The Advanced Country Blocker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'REQUEST_URI' parameter in all versions up to, and including, 2.3.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The injected script is stored via the advcb_live_activity transient on the init hook and executed when an administrator views the Live Monitor page, as the stored URI is unsafely concatenated into a double-quoted HTML title attribute and inserted into the DOM via jQuery .html().	https://plugins.trac.wordpress.org/browser/advanced-country-blocker/tags/2.3.2/advanced-country-blocking.php#L1800 https://plugins.trac.wordpress.org/browser/advanced-country-blocker/tags/2.3.2/advanced-country-blocking.php#L1873 https://plugins.trac.wordpress.org/browser/advanced-country-blocker/tags/2.3.2/advanced-country-blocking.php#L2163 https://www.wordfence.com/threat-intel/vulnerabilities/id/24314e63-df2e-4572-8979-10c6aba0b3d8?source=cve
https://nvd.nist.gov/vuln/detail/cve-2026-123972	**7,2**	The WP-Slimbox2 Plugin plugin for WordPress	Improper Neutralization of Input During Web Page Generation	The WP-Slimbox2 Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'comment' parameter in all versions up to, and including, 1.1.3.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Successful exploitation requires a logged-in user, typically an administrator, to click the attacker's image link in the comment; however, because unmoderated comments appear in the WordPress moderation queue where administrators routinely interact with them, the moderation gate does not meaningfully prevent exploitation. Successful exploitation	https://plugins.trac.wordpress.org/browser/wp-slimbox2/tags/1.1.3.1/index.php#L43 https://plugins.trac.wordpress.org/browser/wp-slimbox2/tags/1.1.3.1/index.php#L83 https://plugins.trac.wordpress.org/browser/wp-slimbox2/tags/1.1.3.1/javascript/slimbox2.js https://plugins.trac.wordpress.org/browser/wp-slimbox2/tags/1.1.3.1/src/slimbox2_autoload.js#L63 https://plugins.trac.wordpress.org/browser/wp-slimbox2/tags/1.1.3.1/src/slimbox2_autoload.js#L79 https://www.wordfence.com/threat-intel/vulnerabilities/id/2d3402c3-d0b6-4226-be05-9b2b2e2bb2b8?source=cve

				causes the attacker's own account to receive the complete Administrator role.	
https://nvd.nist.gov/vuln/detail/cve-2026-125053	**7,2**	WordPress	Improper Neutralization of Input During Web Page Generation	The WEB-Translation – eTranslation Multilingual plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'comment' parameter in all versions up to, and including, 2.0.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The exploit requires that at least one secondary language is configured in the plugin and that comments are open on the target post; because the stored payload contains no literal HTML brackets at save-time, WordPress core KSES filtering does not remove it, and the malicious script is only materialized when a visitor loads the post under a secondary-language URL slug.	https://plugins.trac.wordpress.org/browser/etranslation-multilingual/tags/2.0.7/includes/class-translation-render.php#L307 https://plugins.trac.wordpress.org/browser/etranslation-multilingual/tags/2.0.7/includes/class-translation-render.php#L55 https://www.wordfence.com/threat-intel/vulnerabilities/id/c99aeaaf-d0a3-43a4-bbda-5864c2111746?source=cve
https://nvd.nist.gov/vuln/detail/cve-2026-130737	**7,2**	Grav from 2.0.0	Improper Neutralization of Special Elements	Grav from 2.0.0 before 2.2.18 contains a privilege escalation vulnerability that allows user managers to grant super-admin rights by nesting access maps under a YAML merge key. Attackers with admin.users.create or api.users.write can submit '<<' keys, for example via PATCH /api/v1/users/<self>, that bypass super-grant filtering and gain full site control.	https://github.com/getgrav/grav/security/advisories/GHSA-gm9r-xmhp-p55q
https://nvd.nist.gov/vuln/detail/cve-2026-130758	**7,2**	Fleet	Authorization Bypass Through User-Controlled Key	Fleet before 4.92.0 contains an authorization bypass vulnerability in the deprecated POST /api/latest/fleet/mdm/apple/enqueue endpoint that allows team-scoped users to enqueue Apple MDM commands outside their teams. Attackers with team admin, maintainer, or GitOps roles can include one own-team host UUID alongside unresolved enrollment IDs to send commands like InstallProfile to deleted or user-channel enrollments without activity logging.	https://github.com/fleetdm/fleet/security/advisories/GHSA-5vr5-74q2-mfg4
https://nvd.nist.gov/vuln/detail/cve-2026-115057	**7,1**	Oracle Hyperion Financial	Not specified	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hype-	https://www.oracle.com/security-alerts/cspunov2026.html

				rion (component: Security). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L).	
https://nvd.nist.gov/vuln/detail/cve-2026-115061	**7,1**	Oracle Hyperion Financial	Not specified	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N).	https://www.oracle.com/security-alerts/cspunov2026.html
https://nvd.nist.gov/vuln/detail/cve-2026-115159	**7,1**	Oracle Hyperion Infrastructure	Not specified	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via	https://www.oracle.com/security-alerts/cspunov2026.html

				HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L).	
https://nvd.nist.gov/vuln/detail/cve-2026-115177	**7,1**	Oracle Hyperion Infrastructure	Not specified	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.26.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L).	https://www.oracle.com/security-alerts/cspunov2026.html
https://nvd.nist.gov/vuln/detail/cve-2026-126631	**7,1**	OpenSCAP	Improper Link Resolution Before File Access	A flaw was found in OpenSCAP. This vulnerability allows for information disclosure when performing offline scans of untrusted filesystem images, such as container images or virtual machine (VM) disks. Because the scanner does not properly restrict symbolic link (symlink) resolution to the target image's root directory, an attacker can supply a crafted image containing links pointing to files on the host system. When the scan runs, typically with elevated privileges, OpenSCAP follows these links to read sensitive host	https://access.redhat.com/security/cve/CVE-2026-126631 https://bugzilla.redhat.com/show_bug.cgi?id=2571597

				files and expose their contents in the scan report or manipulate compliance results.	
https://nvd.nist.gov/vuln/detail/cve-2026-127319	**7,1**	Oracle AutoVue	Not specified	Vulnerability in the Oracle AutoVue product of Oracle Supply Chain (component: Security). The supported version that is affected is 21.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle AutoVue. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle AutoVue accessible data as well as unauthorized update, insert or delete access to some of Oracle AutoVue accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).	https://www.oracle.com/security-alerts/cspunov2026.html
https://nvd.nist.gov/vuln/detail/cve-2026-131177	**7,1**	Splunk Enterprise	Improper Neutralization of Special Elements in Output Used by a Downstream Component	In Splunk Enterprise versions below 10.4.4, 10.2.9, 10.0.12, and 9.4.16, a user who does not hold the "admin" or "power" Splunk roles could run arbitrary Search Processing Language (SPL) searches with elevated privileges through saved search dispatch and access stored credentials and indexed data or modify lookup data. The vulnerability is possible because Splunk Enterprise does not correctly neutralize caller-supplied saved search dispatch values before it places the values into an SPL search. For more information see Search endpoint descriptions (https://help.splunk.com/en/splunk-enterprise/leverage-rest-apis/rest-api-reference/10.4/search-endpoints/search-endpoint-descriptions) in the Splunk documentation.	https://advisory.splunk.com/advisories/SVD-2026-1103
https://nvd.nist.gov/vuln/detail/cve-2026-131181	**7,1**	Splunk Enterprise	Improper Neutralization of Special Elements in Data Query Logic	In Splunk Enterprise versions below 10.4.5, 10.2.9, 10.0.12, and 9.4.16, a user who does not hold the "admin" or "power" Splunk roles could use Data Model Acceleration to run malicious Search Processing Language (SPL) commands and perform actions through the	https://advisory.splunk.com/advisories/SVD-2026-1103

				Representational State Transfer (REST) API that the user cannot perform directly. The vulnerability is possible because Splunk Enterprise does not neutralize user-provided data before it adds that data to a generated search. For more information, see Accelerate data models (https://help.splunk.com/en/splunk-enterprise/manage-knowledge-objects/knowledge-management-manual/10.2/use-data-summaries-to-accelerate-searches/accelerate-data-models), Define roles on the Splunk platform with capabilities (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.2/manage-splunk-platform-users-and-roles/define-roles-on-the-splunk-platform-with-capabilities), and About the search language (https://help.splunk.com/en/splunk-enterprise/search/search-manual/10.6/search-overview/about-the-search-language).	
https://nvd.nist.gov/vuln/detail/cve-2026-131198	**7,1**	Splunk Enterprise Security	Improper Input Validation	In Splunk Enterprise Security versions below 8.7.0, a user that holds a role with the mc_view_im_data capability could cause the Mission Control incident mapping Representational State Transfer (REST) API to run arbitrary Search Processing Language (SPL) commands with elevated permissions. With this access, the user could expose all data in Splunk indexes and all stored credentials and modify protected indexes and lookup data. The vulnerability is possible because the Mission Control incident mapping REST API does not validate incident identifiers before including them in SPL searches. For more information see Capability reference for Splunk Enterprise Security (https://help.splunk.com/en/splunk-enterprise-security-8/install/8.7/installation/capability-reference-for-splunk-enterprise-security) and Overview of Mission Control in Splunk Enterprise Security	https://advisory.splunk.com/advisories/SVD-2026-1106

				(https://help.splunk.com/en/splunk-enterprise-security-8/user-guide/8.7/mission-control/overview-of-mission-control-in-splunk-enterprise-security) in the Splunk documentation.	
https://nvd.nist.gov/vuln/detail/cve-2026-131245	**7,1**	Splunk SOAR	Exposure of Sensitive Information to an Unauthorized Actor	In Splunk SOAR versions below 8.8.0, a user with edit permission for the container label of a pending external prompt could obtain the external prompt link through the Representational State Transfer (REST) API and use the link to view and resolve the associated approval. The vulnerability is possible because the approval detail REST API includes the external prompt link in responses outside the assigned approval scope. For more information see REST Approval (https://help.splunk.com/en/splunk-soar/soar-on-premises/rest-api-reference/6.3.1/approval-endpoints/rest-approval), REST External Prompt (https://help.splunk.com/en/splunk-soar/soar-on-premises/rest-api-reference/7.1.0/external-prompt-endpoints/rest-external-prompt), and Manage roles and permissions in Splunk SOAR (On-premises) (https://help.splunk.com/en/splunk-soar/soar-on-premises/administer-soar-on-premises/8.5.0/manage-your-splunk-soar-on-premises-users-and-accounts/manage-roles-and-permissions-in-splunk-soar-on-premises) in the Splunk documentation.	https://advisory.splunk.com/advisories/SVD-2026-1108
https://nvd.nist.gov/vuln/detail/cve-2026-131262	**7,1**	Splunk SOAR	Authorization Bypass Through User-Controlled Key	In Splunk SOAR versions below 8.8.0, an authenticated user who can view and edit containers in at least one container label could create artifacts with parent relationships to containers and artifacts outside those labels. This could expose fields from restricted artifacts and modify incident lineage. The vulnerability is possible because Splunk SOAR does not verify access to the selected parent container and parent artifact when it creates an artifact.	https://advisory.splunk.com/advisories/SVD-2026-1108

https://nvd.nist.gov/vuln/detail/cve-2026-131303	**7,1**	Splunk AI Assistant	Missing Authorization	In Splunk AI Assistant versions below 2.0.0, a user who does not hold the "admin" or "power" Splunk roles could obtain limited information about indexes and data sources outside their authorized scope through the assistant. The vulnerability is possible because Splunk AI Assistant does not fully apply authorization controls to all information that it retrieves.	https://advisory.splunk.com/advisories/SVD-2026-1111
https://nvd.nist.gov/vuln/detail/cve-2026-133306	**7,0**	VideoLAN libaacs 0.7.0	Stack-based Buffer Overflow	VideoLAN libaacs 0.7.0 through 0.12.0 on non-macOS, non-Windows builds contains stack-based buffer overflows in aacs_resolve_path() in src/file/path.c from length checks against the wrong buffer. Local attackers can place a symlink with a long target on a disc path a user opens to overflow resolved_path[] and link[], crashing the process or potentially executing code if mitigations are bypassed.	https://code.videolan.org/videolan/libaacs https://code.videolan.org/videolan/libaacs/-/blob/0.12.0/Makefile.am#L51 https://code.videolan.org/videolan/libaacs/-/blob/0.12.0/src/file/path.c#L127 https://code.videolan.org/videolan/libaacs/-/blob/0.12.0/src/file/path.c#L132 https://code.videolan.org/videolan/libaacs/-/blob/0.12.0/src/file/path.c#L94 https://code.videolan.org/videolan/libaacs/-/blob/0.12.0/src/file/path.c#L97 https://code.videolan.org/videolan/libaacs/-/commit/6bbd2143603b785a9382aa8b20d7f328f7c1400e https://www.vulncheck.com/advisories/videolan-libaacs-0.7.0-through-0.12.0-stack-buffer-overflow-via-aacs-resolve-path

CISA/CERT-EU Alerts & Advisories

Αυτό το κομμάτι περιλαμβάνει ειδοποιήσεις από επίσημες πηγές, κυρίως CISA και CERT-EU, σχετικά με κρίσιμες ευπάθειες ή ενεργές απειλές. Συνήθως αφορούν βιομηχανικά ή κρίσιμα συστήματα, αλλά και mainstream λογισμικό. Προσφέρονται σε μορφή σύντομων αναφορών και οδηγούν σε πιο λεπτομερείς τεχνικές οδηγίες.

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2026-115731 Perforce Puppet Enterprise Deserialization of Untrusted Data Vulnerability	https://www.cisa.gov/news-events/alerts/2026/11/17/cisa-adds-one-known-exploited-vulnerability-catalog
Critical Java Vulnerability Requires Immediate Patching		https://www.cisa.gov/news-events/alerts/2026/11/17/critical-java-vulnerability-requires-immediate-patching

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds Four Known Exploited Vulnerabilities to Catalog	▪ CVE-2024-10441 Synology DiskStation Manager (DSM) Improper Encoding or Escaping of Output Vulnerability ▪ CVE-2026-40217 BerriAI LiteLLM Unprotected Alternate Channel Vulnerability ▪ CVE-2026-90436 Apache Axis Unsafe Reflection Vulnerability ▪ CVE-2026-90817 Vanderbilt University Research Electronic Data Capture (REDCap) Code Injection Vulnerability	https://www.cisa.gov/news-events/alerts/2026/11/18/cisa-adds-four-known-exploited-vulnerabilities-catalog

News

Η ενότητα "News" συνοψίζει τα πιο σημαντικά γεγονότα της εβδομάδας στον τομέα της κυβερνοασφάλειας. Εδώ θα βρείτε επιθέσεις που ξεχώρισαν, νέες τεχνικές που εντοπίστηκαν, ή ενέργειες από γνωστές ομάδες hacking. Δίνει την απαραίτητη εικόνα του τι συμβαίνει διεθνώς και πού πρέπει να στραφεί η προσοχή.

Σύντομη περιγραφή / Τίτλος	URL
Meta AI Agent Muse Reads Encrypted Messages Through Android Notifications and Mac Permissions	https://cybersecuritynews.com/muse-reads-encrypted-messages/
Anthropic Reduces Vulnerability Disclosure Deadline from 90 to 30 Days as AI Quickly Identifies Flaws	https://cybersecuritynews.com/anthropic-cuts-critical-vulnerability-disclosure-deadline/
Russian National Accused of Using Remote Access Tools to Spy on Silicon Valley Defense Firm	https://cybersecuritynews.com/russian-national-silicon-valley-spy/
Microsoft Unveils Windows Server 2028 With Hundreds of Security Protections Enabled by Default	https://cybersecuritynews.com/windows-server-2028-security/
EU Accuses Temu of Failing to Stop Illegal Products, Citing Weak Security and Moderation Controls	https://cybersecuritynews.com/temu-breaching-digital-services-act/
Microsoft Windows 11 Secretly Tracks Which AI Coding Agents Developers Use Through Telemetry	https://cybersecuritynews.com/windows-11-ai-agent-tracking/

Breaches / Compromised / Hacked

Καταγράφονται περιπτώσεις παραβίασης δεδομένων, διαρροών και άλλων σοβαρών περιστατικών ασφαλείας. Περιλαμβάνονται πληροφορίες για το ποιοι επηρεάστηκαν, με ποιον τρόπο έγινε η παραβίαση και πού υπάρχουν διαθέσιμες λεπτομέρειες. Είναι μια χρήσιμη εικόνα για να αντιληφθεί κανείς τη δυναμική των επιθέσεων σε πραγματικές συνθήκες.

Σύντομη περιγραφή / Τίτλος	URL
Hackers Exploit Exposed AI Vendor Key to Breach 10 Barracuda Cloud Accounts in 44 Hours	https://cybersecuritynews.com/barracuda-cloud-accounts/
Microsoft's Agent Framework PyPI Package Hacked to Steal Azure and GitHub Credentials	https://cybersecuritynews.com/microsofts-agent-framework-pypi-package/
Hackers Leak Customer Data Linked to Visa, Mastercard and JPMorgan After Third-Party Cyberattacks	https://cybersecuritynews.com/visa-mastercard-jpmorgan-data-breach/
Google Reveals How Russian Hackers Used One Cloud Breach to Compromise Another US Organization	https://cybersecuritynews.com/russian-hackers-3/
KPMG Canada Confirms Cyberattack as Hackers Access Confidential Client Tax Documents	https://cybersecuritynews.com/kpmg-canada-confirms-cyberattack/
Japan Shuts Down Fugaku Supercomputer After Hackers Breach Internal Servers	https://cybersecuritynews.com/japan-shuts-down-fugaku-supercomputer/
Hackers Hijack Old Bitly Links in Burger King, McDonald's and Trump Posts to Redirect Users	https://cybersecuritynews.com/hackers-hijack-old-bitly-links/
The Gentlemen Ransomware Gang Allegedly Claims to Have Breached NVIDIA	https://cybersecuritynews.com/nvidia-data-breach-claim/
Hackers Target European Commission with ARTEX AI Tool in Major Cyberattack	https://cybersecuritynews.com/european-commission-cyberattack/
N-able Confirms Server Breach, Disables Mail Assure and SpamExperts Management Access	https://cybersecuritynews.com/n-able-confirms-server-breach/
JPMorgan Chase Confirms Third-Party Cyberattack That May Have Exposed Customer Names and Emails	https://cybersecuritynews.com/jpmorgan-third-party-data-breach/

Vulnerabilities / Flaws / Zero-day

Αναφέρονται τεχνικά ελαττώματα ή αδυναμίες που ενδέχεται να αξιοποιηθούν άμεσα από επιτιθέμενους — είτε επειδή είναι zero-day είτε γιατί η διόρθωσή τους καθυστερεί. Περιλαμβάνονται περιπτώσεις όπου δεν απαιτείται αλληλεπίδραση με τον χρήστη ή όπου παρακάμπτονται βασικά μέτρα ασφαλείας. Πολύ χρήσιμο για ομάδες που ασχολούνται με threat detection.

Σύντομη περιγραφή / Τίτλος	URL
Hackers Exploit Unpatched Microsoft Exchange Servers to Deploy Custom RATs Across Southeast Asia	https://cybersecuritynews.com/microsoft-exchange-servers/
CISA Warns Hackers Are Actively Exploiting Four Flaws in Synology, LiteLLM, Apache Axis and REDCap	https://cybersecuritynews.com/flaws-in-synology-litellm-apache-axis-and-redcap/
Critical VMware vCenter Flaws Let Hackers Bypass Authentication and Access Servers	https://cybersecuritynews.com/vmware-vcenter-authentication-bypass/
Ubiquiti Warns of Critical UniFi Access Flaws Enabling Root Code Execution Attacks	https://cybersecuritynews.com/ubiquiti-warns-critical-unifi-access-flaws/
Critical Java4Shell Flaw Lets Hackers Execute Code Without Authentication on OpenJDK Servers	https://cybersecuritynews.com/java4shell/
New phpAfterShell Attack Bypasses PHP2Shell Fix to Enable Remote Code Execution	https://cybersecuritynews.com/phpaftershell-rce/
Critical Apache HTTP Server RCE Vulnerability Actively Exploited in Attacks	https://cybersecuritynews.com/apache-http-server-rce-exploitation/
Microsoft's AI Uncovers 99 Security Issues in Express, ImageMagick and Other Open-Source Projects	https://cybersecuritynews.com/microsofts-ai-uncovers-99-security-issues/
New Hello Again Attack Bypasses Windows Hello and BitLocker PIN Lockout Protection	https://cybersecuritynews.com/hello-attack-bypasses-windows-hello-and-bitlocker/
8.8 Million NGINX Services Still Potentially Exposed to Critical NGINX2Root Vulnerability	https://cybersecuritynews.com/nginx2root-vulnerability/
Hackers Actively Exploit Critical Apache Roller RCE Flaw to Execute Code Without Authentication	https://cybersecuritynews.com/apache-roller-rce-exploitation/
4-Year-Old NVIDIA Linux GPU Flaw Lets Users Hijack Entire Shared Servers	https://cybersecuritynews.com/4-year-old-nvidia-linux-gpu-flaw/
Researchers Break AMD SEV-SNP Security to Read Encrypted Virtual Machine Memory Using a GPU	https://cybersecuritynews.com/amd-sev-snp-security-bypassed/
Hackers Exploiting Java4Shell RCE Flaw Using ARTEX Disguise Themselves as Chrome	https://cybersecuritynews.com/java4shell-rce-flaw-exploited/

Σύντομη περιγραφή / Τίτλος	URL
PHP Security Team Warns of Critical Vulnerabilities, Urges Users to Prepare for November 19 Updates	https://cybersecuritynews.com/php-critical-vulnerabilities/
Hackers Exploit VMware vCenter 0-Day Since September to Hijack Admin Accounts and Steal VM Data	https://cybersecuritynews.com/hackers-exploit-vmware-vcenter-0-day/
CISA Warns of Puppet Enterprise Vulnerability Actively Exploited in Attacks	https://cybersecuritynews.com/puppet-enterprise-flaw-actively-exploited/
PHP Warns of Critical Security Flaws Affecting All Supported Versions, Urges Users to Update	https://cybersecuritynews.com/php-8-released/
NGINX HTTP/2 Flaws Could Allow Memory Corruption and Remote Code Execution on Web Servers	https://cybersecuritynews.com/nginx-http-2-vulnerabilities/
ruby2ßhell: Critical One-Byte Heap Overflow in Ruby Could Allow RCE Attacks	https://cybersecuritynews.com/ruby2shell-rce/
New Windows 11 Narrator Lock Screen 0-Day Allows Attackers to Bypass BitLocker Protections	https://cybersecuritynews.com/windows-11-narrator-lock-screen-0-day/

Patches / Updates / Fixes

Εδώ θα βρείτε τις πιο πρόσφατες διορθώσεις και ενημερώσεις ασφαλείας από προμηθευτές λογισμικού και hardware. Το περιεχόμενο αφορά συγκεκριμένα bugs ή exploits που έχουν ήδη δημοσιοποιηθεί, μαζί με οδηγίες για το πώς να εφαρμοστούν τα patches.

Σύντομη περιγραφή / Τίτλος	URL
Ruby Patches 7 Security Vulnerabilities, Including Buffer Overflow and RCE Flaws	https://cybersecuritynews.com/ruby-patches-7-security-vulnerabilities/
Critical Java 17 RCE Vulnerability Puts Servers at Risk as Oracle Releases 11 Security Fixes	https://cybersecuritynews.com/java-17-rce-vulnerability/
Wireshark 4.6.10 Released With Patch for 39 Security Vulnerabilities	https://cybersecuritynews.com/wireshark-4-6-10-released/
Drupal Fixes Critical RCE Flaw That Could Let Unauthenticated Hackers Take Over Websites	https://cybersecuritynews.com/drupal-fixes-critical-rce-flaw/
Splunk Patches Critical 9.9 RCE and Authentication Bypass Vulnerabilities in SOAR and Enterprise	https://cybersecuritynews.com/splunk-patches-vulnerabilities/
Chrome 158 Fixes 204 Vulnerabilities, Including Critical Code Execution Flaws	https://cybersecuritynews.com/chrome-158-fixes-204-vulnerabilities/

Σύντομη περιγραφή / Τίτλος	URL
Tails Released Emergency Tor Browser Update to fix uBlock Origin Flaw	https://cybersecuritynews.com/tails-tor-browser-update-to-fix-ublock-origin-flaw/
WordPress 7.1.5 Patches 20 Security Issues, Including Potential RCE and SQL Injection Flaws	https://cybersecuritynews.com/wordpress-7-1-5-patches-20-security-issues/
Atlassian Patches 318 Security Vulnerabilities Across Jira, Confluence, Bitbucket and Other Products	https://cybersecuritynews.com/atlassian-patches-318-security-vulnerabilities/

Potential threats / Threat intelligence

Η συγκεκριμένη ενότητα ασχολείται με νέες απειλές, εξελιγμένα malware και τεχνικές επιθέσεων που έχουν εντοπιστεί σε πραγματικές συν-θήκες. Περιλαμβάνονται αναφορές σε εργαλεία που χρησιμοποιούν οι επιτιθέμενοι, αλλά και δείκτες (IoCs) που μπορούν να χρησιμοποιηθούν στην άμυνα.

Σύντομη περιγραφή / Τίτλος	URL
Chinese APT Hackers Target Global Banks to Steal Financial Intelligence and Spy on Microsoft 365 Accounts	https://cybersecuritynews.com/global-banks/
Hackers Impersonate Microsoft Exchange Online Alerts to Trick Users During Microsoft 365 Outage	https://cybersecuritynews.com/hackers-impersonate-microsoft-exchange/
Hackers Use Stolen FortiGate VPN Credentials to Access Corporate Networks and Deploy Custom Malware	https://cybersecuritynews.com/stolen-fortigate-vpn-credentials/
Hackers Impersonate Major Defense Companies to Spread GravityRAT Spyware and Steal Sensitive Data	https://cybersecuritynews.com/spread-gravityrat-spyware/
Hackers Use Fake Shipment ZIP Files and DLL Side-Loading to Deploy PureLogs and PureRAT Malware	https://cybersecuritynews.com/fake-shipment-zip-files-and-dll-side-loading/
Hackers Hijack AI Coding Agents Through Malicious GitHub Repositories to Steal Developer Credentials	https://cybersecuritynews.com/hackers-hijack-ai-coding-agents/
Hackers Steal Exposed AWS Credentials From Docker Hub Images in Just 8 Seconds	https://cybersecuritynews.com/hackers-steal-exposed-aws-credentials/
Malicious iOS Scripts Now Behind 1 in 5 Advertiser Suspensions as Coruna Exploit Kit Hides Inside Ad Landing Pages	https://cybersecuritynews.com/malicious-ios-scripts-now-behind-1-in-5-advertiser-suspensions-as-coruna-exploit-kit-hides-inside-ad-landing-pages/
TheMailer – Self-hosted Phishing Platform that Runs on Claude and ChatGPT	https://cybersecuritynews.com/themailer-ai-phishing-platform/

Σύντομη περιγραφή / Τίτλος	URL
Hackers Target US Trucking Companies With Fake Freight Portals to Steal Credentials and Deploy Malware	https://cybersecuritynews.com/fake-freight-portals/
Hackers Abuse Microsoft SharePoint and GitHub to Hide Graph-Door Backdoor Attacks on Government Networks	https://cybersecuritynews.com/graphdoor-sharepoint-backdoor/
AI Hacking Framework CyberStrikeAI Runs 221 Tool Executions Without Human Approval	https://cybersecuritynews.com/cyberstrikeai/
AuditTeam Ransomware Gang Poses as Security Auditors and Use AV Drivers to Kill EDR Process	https://cybersecuritynews.com/auditteam-ransomware-gang/
Hackers Deploy Overlord RAT That Survives Windows Resets and Crashes Systems When Terminated	https://cybersecuritynews.com/hackers-deploy-overlord-rat/
Hackers Abuse CyberPower UPS Software to Execute SYSTEM Commands and Dump Active Directory Data	https://cybersecuritynews.com/hackers-abuse-cyberpower-ups-software/
Hackers Turn aNotepad Into a Malware Delivery Channel for Xeno-RAT and NodeLinkRAT Backdoors	https://cybersecuritynews.com/hackers-turn-anotepad/
Chinese Hackers Upgrade EggStreme Malware With Silent Back-door to Evade Security Detection	https://cybersecuritynews.com/eggstreme-malware/
Fake FMCSA, DAT, and TIMOCOM Portals Attack US Logistics Firms	https://cybersecuritynews.com/fake-fmcsa-dat-timocom-portals-target-us-logistics/
Hackers Exploit Microsoft 365 Device Code Authentication to Hi-jack Accounts and Bypass MFA	https://cybersecuritynews.com/device-code-authentication/
Hackers Use Hidden Cron Jobs to Reinstall Malware on Firewalls and Routers Every 5 Minutes	https://cybersecuritynews.com/hackers-use-hidden-cron-jobs/
FBI Warns Hackers Abuse Google Search to Spread Gootloader Malware and Launch Ransomware Attacks	https://cybersecuritynews.com/spread-gootloader-malware/
Hackers Steal US Bank, IRS and Social Security Login Credentials From Infected Computers	https://cybersecuritynews.com/hackers-steal-us-bank/
BADBOX 3.0 Malware Infects Android TV Boxes to Generate 40 Bil-lion Fraudulent Ad Requests Daily	https://cybersecuritynews.com/badbox-3-0-malware/
Hackers Use GhostMap eBPF Rootkit to Hide IronWorm Malware From Linux Security Tools	https://cybersecuritynews.com/hackers-use-ghostmap-ebpf-rootkit/

Guides / Tools

Παρουσιάζονται τεχνικοί οδηγοί και εργαλεία που μπορούν να βοηθήσουν στην παρακολούθηση, ανάλυση ή ενίσχυση της ασφάλειας συστημάτων. Είτε πρόκειται για open source projects είτε για νέες τεχνικές, η ενότητα αυτή λειτουργεί ως πόρος για πρακτικές λύσεις στην καθημερινή δουλειά των επαγγελματιών ασφάλειας.

Σύντομη περιγραφή / Τίτλος	URL
Flipper Devices Launches Flipper One Linux-based Multi-tool With Advanced Network Security Tools	https://cybersecuritynews.com/flipper-one-linux-multi-tool/

References

[1]. Ο βαθμός επικινδυνότητας είναι σύμφωνα με την κλίμακα Common Vulnerability Scoring System (CVSSv3), https://nvd.nist.gov/vuln-metrics/cvss

[2]. Τα CVEs αποτελέσματα που εμφανίζονται στην ενότητα 1 διαθέτουν CVSS v3.1 score >= 7.0 και αφορούν το διάστημα 24/10/2026–27/10/2026.

Annex – Websites with vendor specific vulnerabilities

Ο πίνακας περιέχει websites από κατασκευαστές που προσφέρουν πληροφορίες σχετικές με ευπάθειες που εμφανίζονται στα προϊόντα τους.

Vendor name / Platform	URL
Wordpress	Wordfence Intelligence Vulnerability Database API https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/ Scan your WordPress website, https://wpscan.com/scan/
Oracle	Critical Patch Updates, Security Alerts and Bulletins, https://www.oracle.com/security-alerts/
Fortinet	Fortinet products, https://www.fortiguard.com/psirt
IBM	Security bulletins, https://cloud.ibm.com/status/security Research, Collaborate and Act on threat intelligence, https://exchange.xforce.ibmcloud.com/
MS Windows	The Microsoft Security Response Center (MSRC), https://msrc.microsoft.com/update-guide/
SAP	SAP Security Notes, https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html
Dell	Security Advisories, Notices and Resources, https://www.dell.com/support/security/en-us
HPE	HPE Security Bulletin Library, https://support.hpe.com/connect/s/securitybulletinlibrary Security Bulletins, https://support.hp.com/us-en/security-bulletins
Cisco	Cisco Security Advisories, https://sec.cloudapps.cisco.com/security/center/publicationListing.x
Palo Alto	Palo Alto Networks Security Advisories, https://security.paloaltonetworks.com/
Ivanti	Security Advisory, https://www.ivanti.com/blog/topics/security-advisory
Mozilla	Mozilla Foundation Security Advisories, https://www.mozilla.org/en-US/security/advisories/
Android	Android Security Bulletins, https://source.android.com/docs/security/bulletin/asb-overview
Zyxel	Security Advisories, https://www.zyxel.com/global/en/support/security-advisories
D-Link	Global Security Advisories, Responses, and Notices, https://supportannouncement.us.dlink.com/
Adobe	Security Bulletins and Advisories, https://helpx.adobe.com/security/security-bulletin.html
Siemens	Siemens ProductCERT and Siemens CERT, https://www.siemens.com/global/en/products/services/cert.html
Splunk	Splunk Security Advisories, https://advisory.splunk.com/