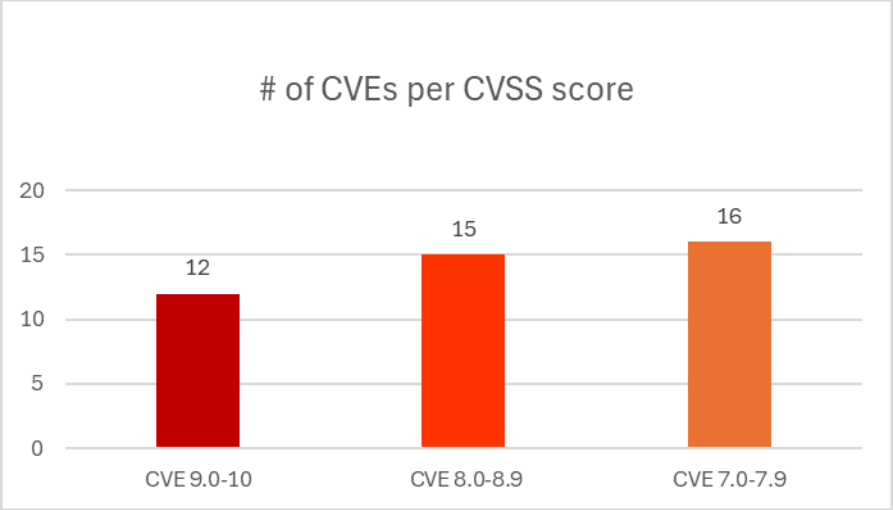
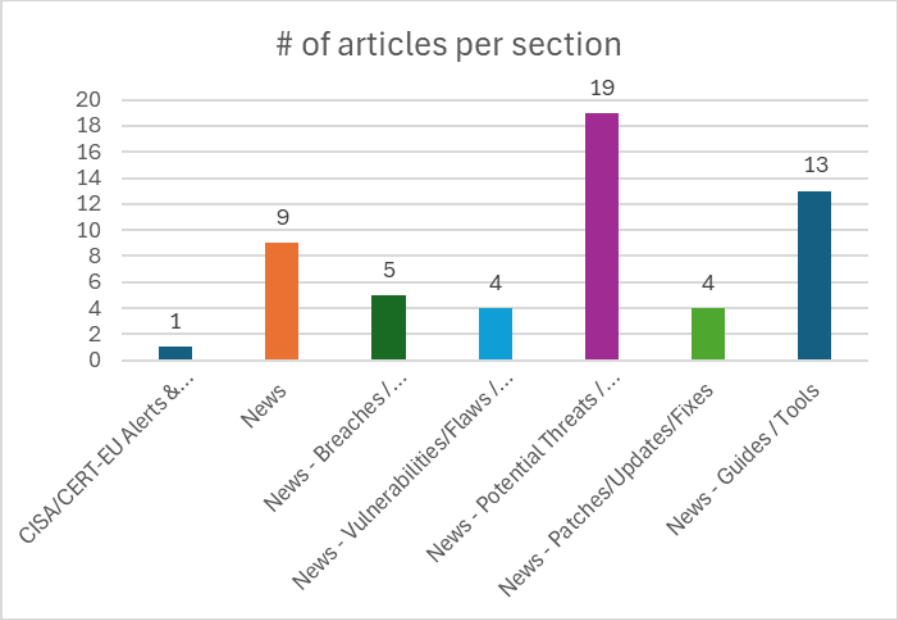


Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 14/11/2026 - 17/11/2026





Contents

Common Vulnerabilities and Exposures (CVEs) 3
CISA/CERT-EU Alerts & Advisories 13
News 14
Breaches / Compromised / Hacked 15
Vulnerabilities / Flaws / Zero-day 15
Patches / Updates / Fixes 16
Potential threats / Threat intelligence 16
Guides / Tools 18
References 19
Annex – Websites with vendor specific vulnerabilities 20

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-2026-129351	10,0	TRENDnet	Improper Restriction of Operations within the Bounds of a Memory Buffer; Out-of-bounds Write	A security vulnerability has been detected in TRENDnet TEW-657BRM 1.00.1. This vulnerability affects the function sprintf of the file /setup.cgi of the component mini_httpd. Such manipulation leads to out-of-bounds write. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. The vendor explains: ""I am not able to confirm if such vulnerability exists as the product has been EOL for more than 15 years. We will send out an announcement letting customers know." This vulnerability only affects products that are no longer supported by the maintainer.	https://github.com/ruanyi101/router-firmware-security-advisories/blob/main/router-firmware-GitHub-advisories/advisories/TRENDnet-TEW-657BRM-mini_httpd.md https://vuldb.com/cve/CVE-2026-129351 https://vuldb.com/submit/1043518 https://vuldb.com/vuln/437397 https://vuldb.com/vuln/437397/cti
https://nvd.nist.gov/vuln/detail/cve-2026-129354	10,0	D-Link DIR-600L	Improper Restriction of Operations within the Bounds of a Memory Buffer; Stack-based Buffer Overflow	A flaw has been found in D-Link DIR-600L 2.17b02. Affected by this issue is the function hnap_main of the file htdocs/cgibin of the component HNAP Handler. Executing a manipulation can lead to stack-based buffer overflow. The attack can be executed remotely. The exploit has been published and may be used.	https://github.com/ruanyi101/router-firmware-security-advisories/blob/main/router-firmware-GitHub-advisories/advisories/D-Link-DIR-600L-HNAP-SOAPAction.md https://vuldb.com/cve/CVE-2026-129354 https://vuldb.com/submit/1043526 https://vuldb.com/vuln/437417 https://vuldb.com/vuln/437417/cti https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/cve-2026-129451	9,9	DrayTek Vigor	Improper Limitation of a Pathname to a Restricted Directory	A flaw has been found in DrayTek Vigor2960 up to 1.5.1.6. This affects the function app_guest_export of the file /cgi-bin/mainfunction.cgi. This manipulation of the argument filename causes path traversal. 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. The affected component should be upgraded. 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/DRV2960-0017-authenticated-app-guest-export-path-traversal-write-delete https://vuldb.com/cve/CVE-2026-129451 https://vuldb.com/submit/1044961 https://vuldb.com/vuln/437462 https://vuldb.com/vuln/437462/cti

https://nvd.nist.gov/vuln/detail/cve-2026-17408	9,8	IBM API Connect	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2	https://www.ibm.com/support/pages/node/7295635 https://www.ibm.com/support/pages/node/7295637
https://nvd.nist.gov/vuln/detail/cve-2026-129952	9,8	NodePress	Use of Default Cryptographic Key	NodePress through 8.5.1 contains an authentication bypass vulnerability that allows unauthenticated remote attackers to gain administrator access by forging JWTs with the hardcoded 'nodepress-secret' fallback key. Attackers can sign HS256 bearer tokens with the default issuer, audience, and role 'admin' to access administrator-only APIs for article, comment, options, and file management.	https://github.com/surmon-china/nodepress/blob/v8.5.1/src/app.config.ts#L62-L72 https://github.com/surmon-china/nodepress/blob/v8.5.1/src/core/auth/auth.module.ts#L17-L29 https://github.com/surmon-china/nodepress/blob/v8.5.1/src/main.ts#L44-L60 https://github.com/surmon-china/nodepress/issues/143 https://www.vulncheck.com/advisories/nodepress-through-8.5.1-authentication-bypass-via-default-jwt-signing-secret
https://nvd.nist.gov/vuln/detail/cve-2026-129955	9,8	NodePress	Use of Default Credentials	NodePress through 8.5.1 contains an authentication bypass vulnerability that allows unauthenticated attackers to gain administrator access by using the hardcoded default password 'root'. Attackers can send base64-encoded 'root' to POST /admin/login when NP_ADMIN_DEFAULT_PASSWORD is unset to obtain admin tokens and fully control the site.	https://github.com/surmon-china/nodepress/blob/v8.5.1/src/app.config.ts#L62-L64 https://github.com/surmon-china/nodepress/blob/v8.5.1/src/modules/admin/admin.service.auth.ts#L45-L58 https://github.com/surmon-china/nodepress/blob/v8.5.1/src/modules/admin/admin.service.profile.ts#L48-L64 https://github.com/surmon-china/nodepress/issues/143 https://www.vulncheck.com/advisories/nodepress-through-8.5.1-authentication-bypass-via-default-administrator-password
https://nvd.nist.gov/vuln/detail/cve-2026-130071	9,8	TridotsTech	Missing Authentication for Critical Functionality	TridotsTech go1cms master branch through commit 7f68d05 and version-3 branch before commit ead8da3 contains a missing authentication vulnerability in the guest-whitelisted update_doc method that allows unauthenticated attackers to modify any document. Attackers can supply a doctype, name and arbitrary fields that are saved with ignore_permissions=True, altering User records to escalate privileges, take over accounts or tamper with business data.	https://github.com/TridotsTech/go1cms/blob/7f68d05502ef88f6ea7190ddf4e1a46314ed75b0/go1_cms/go1_cms/doctype/web_page_builder/web_page_builder.py#L2358-L2378 https://github.com/TridotsTech/go1cms/commit/ead8da36a9452b961cc5361d6fd853ca68a58b08 https://www.vulncheck.com/advisories/tridotstech-go1cms-unauthenticated-arbitrary-document-modification-via-update-doc
https://nvd.nist.gov/vuln/detail/cve-2026-79614	9,8	Zyxel DX3301-T0	Out-of-bounds Write	An out-of-bounds write vulnerability in “libclinkc.so” in Zyxel DX3301-T0/EX3301-T0 firmware versions through 5.50(ABVY.8.3)C0 could allow an unauthenticated attacker to elevate privileges and potentially execute arbitrary commands by sending a crafted HTTP request. WAN access is disabled by default on these devices.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-out-of-bounds-write-and-post-authentication-command-injection-vulnerabilities-in-certain-dsl-ethernet-cpe-fiber-onts-and-wireless-extenders-11-17-2026
https://www.cve.org/CVERecord?id=CVE-2026-120868	9,3	Citrix NetScaler	Improper Restriction of Operations within the Bounds of a Memory Buffer	Memory overflow in Packet Processing can lead to unpredictable or erroneous behavior or Denial of Service in NetScaler ADC and NetScaler Gateway.	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697305

https://nvd.nist.gov/vuln/detail/cve-2026-129452	9,1	DrayTek Vigor	Improper Neutralization of Special Elements in Output Used by a Downstream Component; Improper Neutralization of Special Elements used in a Command	A vulnerability has been found in DrayTek Vigor2960 1.5.1.6. This vulnerability affects the function set_table of the file /cgi-bin/mainfunction.cgi. Such manipulation of the argument jsondata leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.5.1.7 is able to resolve this issue. It is suggested to 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/DRV2960-0019-authenticated-set-table-config-field-command-injection https://vuldb.com/cve/CVE-2026-129452 https://vuldb.com/submit/1044962 https://vuldb.com/vuln/437463 https://vuldb.com/vuln/437463/cti
https://nvd.nist.gov/vuln/detail/cve-2026-129483	9,1	Cyrus SASL	Improper Authentication	Cyrus SASL through 2.1.28 contains an authentication bypass vulnerability in the SRP server mechanism because srp_server_mech_step2 does not reject client public values A that are multiples of N. Unauthenticated network clients can send A equal to N to force a zero shared secret, authenticating as any existing user without the password and learning session keys.	https://gist.github.com/afldl/18d15d3f5a1df99411e35000c7de80db https://github.com/cyrusimap/cyrus-sasl/blob/cyrus-sasl-2.1.28/plugins/srp.c#L2046-L2050 https://github.com/cyrusimap/cyrus-sasl/commit/fb3724f43dc50247ff2bf02135457d6d77031654 https://github.com/cyrusimap/cyrus-sasl/issues/896 https://seclists.org/oss-sec/2026/q4/122 https://www.vulncheck.com/advisories/cyrus-sasl-through-2.1.28-srp-authentication-bypass-via-plugins-srp-c
https://nvd.nist.gov/vuln/detail/cve-2026-130072	9,1	Cloud Commander	Missing Authentication for Critical Functionality	Cloud Commander (cloudcmd) before 19.21.4 contains an authentication bypass and path traversal vulnerability that allows unauthenticated attackers to rename files by sending PUT /rename requests handled before authentication middleware. Attackers can supply absolute or ../ paths in the from and to arrays to move any file the Node.js process can access outside the configured root, causing data loss or denial of service.	https://github.com/coderaiser/cloudcmd/blob/v19.21.2/server/cloudcmd.js#L253-L258 https://github.com/coderaiser/cloudcmd/commit/25f496ff1c0d512354de92cb7f76c6e86c16aa8f https://github.com/coderaiser/cloudcmd/issues/486 https://github.com/coderaiser/cloudcmd/releases/tag/v19.21.4 https://www.vulncheck.com/advisories/cloud-commander-before-19.21.4-authentication-bypass-and-path-traversal-via-put-rename
https://nvd.nist.gov/vuln/detail/cve-2026-129255	9,1	CoolerMaster	Incorrect Privilege Assignment; Incorrect Default Permissions	A vulnerability was identified in CoolerMaster MASTERPLUS+ 1.9.6. This affects the function sub_11504 in the library WinRing0x64.sys of the component Device Driver. The manipulation of the argument PhysicalAddress leads to incorrect default permissions. The attack can only be performed from a local environment. The vendor was contacted early about this disclosure but did not respond in any way.	https://vuldb.com/cve/CVE-2026-129255 https://vuldb.com/submit/1042970 https://vuldb.com/vuln/437286 https://vuldb.com/vuln/437286/cti

https://nvd.nist.gov/vuln/detail/cve-2026-129545	8,8	Kalmia	Improper Privilege Management	Kalmia through 0.2.0 contains a privilege escalation vulnerability that allows low-privileged authenticated users to modify any account via the /kal-api/auth/user/edit endpoint. Attackers holding only read permission can set their admin flag and 'all' permission or reset an administrator's password to fully take over the instance.	https://github.com/DifuseHQ/Kalmia https://github.com/DifuseHQ/Kalmia/blob/1bc059450c3901b17e1be99209965b12f6d163e4/services/auth.go#L183-L232 https://github.com/DifuseHQ/Kalmia/issues/35 https://www.vulncheck.com/advisories/kalmia-through-0.2.0-privilege-escalation-via-kal-api-auth-user-edit
https://nvd.nist.gov/vuln/detail/cve-2026-129948	8,8	Contentlayer	Improper Neutralization of Directives in Dynamically Evaluated Code	Contentlayer @contentlayer/source-files through 0.3.4 contains a code injection vulnerability that allows attackers who control content files to execute JavaScript by abusing gray-matter's still-enabled JavaScript engine in parseMarkdown(). Attackers can start a Markdown or MDX file with a ---js or ---javascript frontmatter delimiter to run code during build, exposing CI build secrets.	https://github.com/contentlayerdev/contentlayer/blob/v0.3.4/packages/@contentlayer/source-files/src/fetchData/makeCacheItemFromFilePath.ts#L221-L228 https://github.com/contentlayerdev/contentlayer/issues/688 https://www.vulncheck.com/advisories/contentlayer-contentlayer-source-files-through-0.3.4-code-injection-via-javascript-frontmatter
https://nvd.nist.gov/vuln/detail/cve-2026-130082	8,8	PostgreSQL	Improper Neutralization of Special Elements used in an SQL Command	django-tenants 3.4.8 before 4.0.1 contains an SQL injection vulnerability in its PostgreSQL backend that allows attackers to inject SQL through unescaped tenant schema names. Attackers who can choose or influence a schema name can supply quote characters that are interpolated into SET search_path and CREATE, DROP or ALTER SCHEMA statements, letting them read other tenants' data or run SQL as the application's database user.	https://github.com/django-tenants/django-tenants/blob/v4.0.0/django_tenants/postgresql_backend/base.py#L208-L213 https://github.com/django-tenants/django-tenants/blob/v4.0.0/django_tenants/postgresql_backend/base.py#L46 https://github.com/django-tenants/django-tenants/commit/46d89c0fccc820f88657e6ec152ba855072571ff https://github.com/django-tenants/django-tenants/releases/tag/v4.0.1 https://github.com/django-tenants/django-tenants/security/advisories/GHSA-693j-7v9f-x7pw https://www.vulncheck.com/advisories/django-tenants-3.4.8-before-4.0.1-sql-injection-via-unescaped-schema-name
https://nvd.nist.gov/vuln/detail/cve-2026-130361	8,8	AdminNeo	Improper Neutralization of Argument Delimiters in a Command	AdminNeo before 5.9.1 contains a parameter injection vulnerability in its ClickHouse driver that allows attackers to inject ClickHouse HTTP query parameters through an unencoded db GET parameter. Attackers can lure a logged-in victim into opening a crafted GET link that injects a query parameter, bypassing the POST-only CSRF token. ClickHouse then executes attacker-chosen SQL under the victim's credentials to read, modify, or drop data.	https://github.com/adminneo-org/adminneo/releases/tag/v5.9.1 https://github.com/adminneo-org/adminneo/security/advisories/GHSA-gj7f-g8j2-wxxr https://www.vulncheck.com/advisories/adminneo-before-5.9.1-clickhouse-http-parameter-injection-via-db-parameter

https://nvd.nist.gov/vuln/detail/cve-2026-130382	8,8	OtpLoginPlugin	Authentication Bypass Using an Alternate Path or Channel	AdminNeo before 5.9.1 contains an authentication bypass vulnerability in OtpLoginPlugin that allows attackers knowing the database password to skip TOTP verification by abusing the permanent-login cookie. Attackers can submit a login with a wrong OTP and permanent=1 to obtain a neo_permanent cookie, then replay it to gain full authenticated database access.	https://github.com/adminneo-org/adminneo/releases/tag/v5.9.1 https://github.com/adminneo-org/adminneo/security/advisories/GHSA-xwpg-q47q-pg26 https://www.vulncheck.com/advisories/adminneo-before-5.9.1-totp-authentication-bypass-via-neo-permanent-cookie
https://nvd.nist.gov/vuln/detail/cve-2026-130073	8,8	CBoard before commit 7bd8180	Missing Authorization	CBoard before commit 7bd8180 contains a missing authorization vulnerability that allows any authenticated user to reach admin functions because AdminController and DashboardController methods bypass AOP role checks. Attackers with no role grants can call deleteUser, deleteRole, getUserList, getAllWidgetList and getAllDatasetList to read query configurations and delete accounts including the administrator.	https://github.com/Tui-Qiao/CBoard/blob/046914c785eca1c1f91a8887ce36f1c2b34f25f6/src/main/java/org/cboard/controller/AdminController.java#L72-L98 https://github.com/Tui-Qiao/CBoard/blob/046914c785eca1c1f91a8887ce36f1c2b34f25f6/src/main/java/org/cboard/services/role/ConfigRuleService.java#L135-L158 https://github.com/TuiQiao/CBoard/commit/7bd8180d8423a36b29a803433078bd66f94a81ed https://github.com/TuiQiao/CBoard/issues/740 https://www.vulncheck.com/advisories/cboard-before-commit-7bd8180-missing-authorization-in-admin-and-dashboard-endpoints
https://nvd.nist.gov/vuln/detail/cve-2026-129261	8,3	Kingston	Exposed IOCTL with Insufficient Access Control	A vulnerability was found in Kingston FURY CTRL RGB Control Software up to 2.0.66.0. The impacted element is an unknown function in the library NTIOLib_X64.sys of the component IOCTL Handler. Performing a manipulation results in exposed ioctl with insufficient access control. The attack is only possible with local access.	https://vuldb.com/cve/CVE-2026-129261 https://vuldb.com/submit/1043190 https://vuldb.com/vuln/437302 https://vuldb.com/vuln/437302/cti
https://nvd.nist.gov/vuln/detail/cve-2026-129445	8,2	D-Link DIR-850L FW1	Use of Hard-coded Password; Use of Hard-coded Credentials	A security flaw has been discovered in D-Link DIR-850L FW1.20WWb03. This impacts an unknown function of the file /usr/sbin/consolepwd of the component Console Login. Performing a manipulation results in hard-coded credentials. The attack requires a local approach. The exploit has been released to the public and may be used for attacks.	https://github.com/XueDugu/dlink-dir850l-consolepwd-evidence https://vuldb.com/cve/CVE-2026-129445 https://vuldb.com/submit/1044944 https://vuldb.com/vuln/437458 https://vuldb.com/vuln/437458/cti https://www.dlink.com/

https://nvd.nist.gov/vuln/detail/cve-2026-121684	8,2	The Soledad theme for WordPress	Improper Neutralization of Special Elements in Output Used by a Downstream Component	The Soledad theme for WordPress is vulnerable to unauthenticated Remote Code Execution in versions up to, and including, 8.7.7 The public penci_more_post_ajax AJAX action feeds infeedads[ads_code] (base64+urldecoded) to penci_safe_shortcode(), whose allowlist regex inspects only the hyphen-truncated outer shortcode name (e.g. 'adinserter') and never the nested [elementor-element k=.. data=..] tag, so do_shortcode() renders an attacker-chosen Elementor element. The rendered penci-featured-sliders widget passes its unsanitized 'style' setting to include dirname(__FILE__)."/{$style}.php", a path-traversal local file inclusion.	https://themeforest.net/item/soledad-multiconcept-blogmagazine-wp-theme/12945398 https://www.wordfence.com/threat-intel/vulnerabilities/id/bb3fe92d-adf8-4ab7-bc1a-9cf78ea4412f?source=cve
https://nvd.nist.gov/vuln/detail/cve-2026-130074	8,1	ChangePasswordInfo handler	Authorization Bypass Through User-Controlled Key	free5GC WebConsole through 1.4.6 contains an authorization flaw in the ChangePasswordInfo handler that allows authenticated tenant users to change other members' passwords. Attackers can send POST /api/change-password with another tenant member's email and a new password, without the current password, to take over that account.	https://github.com/free5gc/webconsole/blob/v1.4.6/backend/WebUI/api_webui.go#L2220-L2270 https://github.com/free5gc/webconsole/commit/615b4105eb6a7a606b1e0416ccde293877044c05 https://github.com/free5gc/webconsole/issues/243 https://www.vulncheck.com/advisories/free5gc-webconsole-through-1.4.6-account-takeover-via-api-change-password
https://nvd.nist.gov/vuln/detail/cve-2026-130366	8,1	ClickHouse driver	Improper Authentication	AdminNeo before 5.9.1 contains an authentication bypass vulnerability in the ClickHouse driver that allows remote attackers to log in to passwordless accounts without the configured defaultPasswordHash password. Attackers who know the name of a ClickHouse no_password account can submit any non-empty password, because connect() skips openPasswordless(), and obtain a session with that account's rights.	https://github.com/adminneo-org/adminneo/commit/7905a3583d25ccfa598665d717dd722e4f7ce52e https://github.com/adminneo-org/adminneo/releases/tag/v5.9.1 https://github.com/adminneo-org/adminneo/security/advisories/GHSA-h9x9-p972-28q9 https://www.vulncheck.com/advisories/adminneo-before-5.9.1-authentication-bypass-via-clickhouse-driver-defaultpasswordhash
https://nvd.nist.gov/vuln/detail/cve-2026-130369	8,1	phpMyFAQ	Authorization Bypass Through User-Controlled Key	phpMyFAQ 4.1.9 before 4.1.12 and 4.2.0-alpha before 4.2.0-RC.2 contains an authorization bypass vulnerability in multisite deployments that allows attackers to overwrite passkeys of accounts on other tenants via a shared PHP session store. Attackers can run WebAuthn prepare() for a login on one tenant, then replay the session against /api/webauthn/register on another tenant or the master to replace that user's passkeys and log in as admin.	https://github.com/thorsten/phpMyFAQ/commit/8a7eeddddda7f11882d1e9944ab92473c6890b85 https://github.com/thorsten/phpMyFAQ/releases/tag/4.1.12 https://github.com/thorsten/phpMyFAQ/releases/tag/4.2.0-RC.2 https://github.com/thorsten/phpMyFAQ/security/advisories/GHSA-j82j-jp9w-f75c https://www.vulncheck.com/advisories/phpmyfaq-4.1.9-before-4.1.12-and-4.2.0-alpha-before-4.2.0-rc.2-cross-tenant-webauthn-account-takeover

https://nvd.nist.gov/vuln/detail/cve-2026-130371	8,1	phpMyFAQ	Missing Authentication for Critical Functionality	phpMyFAQ before 4.1.12 and 4.2.0-alpha before 4.2.0-RC.2 contains an authentication bypass vulnerability because the web installer ignores the legacy config/database.php during 3.x upgrades. Unauthenticated attackers can reinstall the site against an attacker-controlled database and create their own administrator account to take over the application.	https://github.com/thorsten/phpMyFAQ/commit/eae6674d64bb6f53caf703d3f38b657f0c16a13c https://github.com/thorsten/phpMyFAQ/releases/tag/4.1.12 https://github.com/thorsten/phpMyFAQ/releases/tag/4.2.0-RC.2 https://github.com/thorsten/phpMyFAQ/security/advisories/GHSA-jhf3-22r2-88hm https://www.vulncheck.com/advisories/phpmyfaq-before-4.1.12-and-4.2.0-alpha-before-4.2.0-rc.2-unauthenticated-reinstall-via-web-installer
https://nvd.nist.gov/vuln/detail/cve-2026-130380	8,1	AdminNeo	Authentication Bypass Using an Alternate Path or Channel	AdminNeo before 5.9.1 contains an authentication bypass vulnerability in the sqlsrv-based MS SQL driver that allows unauthenticated attackers to log in by submitting an empty username. Attackers can supply any non-empty password, triggering Windows integrated authentication that grants a full session with the web server identity's SQL Server privileges.	https://github.com/adminneo-org/adminneo/releases/tag/v5.9.1 https://github.com/adminneo-org/adminneo/security/advisories/GHSA-w8j4-8pww-wm83 https://www.vulncheck.com/advisories/adminneo-before-5.9.1-authentication-bypass-via-ms-sql-empty-username
https://nvd.nist.gov/vuln/detail/cve-2026-124019	8,1	VB-Audio VB-CABLE	Out-of-bounds Read; Out-of-bounds Write	VB-Audio VB-CABLE virtual audio device kernel streaming driver (vbaudio_cable64_win10.sys 10.0.10011.16384) contains out-of-bounds read and write vulnerabilities in its KSPROPSETID_Audio MUTE, VOLUMELEVEL, and PEAKMETER2 property handlers that allow a local standard user to supply an all-channels sentinel value which is improperly used as a loop terminator or array index instead of being bounds-checked. Attackers can exploit the accessible low-integrity KS filter device object to write attacker-controlled values sequentially into kernel memory corrupting kernel globals and object pointers, or read past an array boundary to leak kernel memory, resulting in local privilege escalation or denial of service via a kernel bug check.	https://vb-audio.com/Cable/index.htm https://www.vulncheck.com/advisories/vb-audio-vb-cable-kernel-driver-out-of-bounds-write
https://nvd.nist.gov/vuln/detail/cve-2026-129956	8,0	SbieSvc	Improper Privilege Management	Sandboxie-Plus before 1.18.6 contains a local privilege escalation vulnerability in SbieSvc that allows standard users to launch UpdUtil.exe as SYSTEM via MSGID_PROCESS_RUN_UPDATER requests. Attackers can inject code into a signed SandMan.exe process to bypass the signature check and write attacker-controlled files to arbitrary paths, achieving SYSTEM code execution.	https://github.com/sandboxie-plus/Sandboxie/blob/v1.18.5/Sandboxie/core/svc/ProcessServer.cpp#L1519-L1611 https://github.com/sandboxie-plus/Sandboxie/blob/v1.18.5/SandboxieTools/UpdUtil/UpdUtil.cpp#L1349-L1386 https://github.com/sandboxie-plus/Sandboxie/commit/4e121cc4dacdc31973adcb81581b0414d48c26fc https://github.com/sandboxie-plus/Sandboxie/releases/tag/v1.18.6 https://github.com/sandboxie-plus/Sandboxie/security/advisories/GHSA-46vh-v2q6-wrcv https://www.vulncheck.com/advisories/sandboxie-plus-before-1.18.6-privilege-escalation-via-sbiesvc-msgid-process-run-updater

https://nvd.nist.gov/vuln/detail/cve-2026-130067	7,8	7-Zip File Manager	User Interface (UI) Misrepresentation of Critical Information	7-Zip File Manager before 26.03 fails to detect archive entry names padded with Unicode space characters, allowing attackers to bypass the deceptive file name warning in CPanel::IsVirus_Message. Attackers can craft archive entries like a PDF name followed by ideographic spaces and .hta to hide the real extension, executing script content via ShellExecuteExW when opened.	https://github.com/ip7z/7zip/blob/26.02/CPP/7zip/UI/FileManager/PanelItemOpen.cpp#L867-L893 https://github.com/ip7z/7zip/commit/0766b733fe3e06dd2a7f9a3cfbf2108ac73abd17 https://github.com/ip7z/7zip/releases/tag/26.03 https://www.7-zip.org/history.txt https://www.vulncheck.com/advisories/7-zip-file-manager-before-26.03-file-name-spoofing-warning-bypass-via-unicode-spaces
https://nvd.nist.gov/vuln/detail/cve-2026-129880	7,8	DeepAudit 2.0.0-beta.5	Server-Side Request Forgery	DeepAudit 2.0.0-beta.5 through 3.8.0 contains a server-side request forgery vulnerability that allows registered users to leak server-wide GitLab or Gitea tokens via repository_url. Attackers can create a gitlab or gitea project pointing to a controlled host and request its branches to capture the operator's token and reach internal hosts.	https://github.com/lintsinghua/DeepAudit/blob/9aa46568f20b2ab2dbc1878a4479392012c1230a/backend/app/api/v1/endpoints/projects.py#L720-L760 https://github.com/lintsinghua/DeepAudit/blob/9aa46568f20b2ab2dbc1878a4479392012c1230a/backend/app/services/scanner.py#L122-L152 https://github.com/lintsinghua/DeepAudit/blob/9aa46568f20b2ab2dbc1878a4479392012c1230a/backend/app/utils/repo_utils.py#L38-L68 https://vul.yulun.ac.cn/20261106/deepaudit/ https://www.vulncheck.com/advisories/deepaudit-2.0.0-beta.5-through-3.8.0-ssrf-via-project-branch-listing-leaks-git-tokens
https://nvd.nist.gov/vuln/detail/cve-2026-12487	7,8	SNMP parameter of Zyxel EE5301-00 customized firmware	Incorrect Authorization	An incorrect authorization vulnerability in the SNMP parameter of Zyxel EE5301-00 customized firmware version 5.63(ACLD.2)b3_D0 could allow an unauthenticated attacker to cause a denial-of-service (DoS) condition on an affected device.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-incorrect-authorization-vulnerability-in-the-snmp-parameter-of-customized-firmware-for-the-ee5301-00-ethernet-cpe-11-17-2026
https://nvd.nist.gov/vuln/detail/cve-2026-127218	7,7	Axigen Mail Server 10.3.3.67	Uncontrolled Recursion	Axigen Mail Server 10.3.3.67 through 10.3.3.x, 10.4.42 through 10.4.x, 10.5.29 through 10.5.x, 10.6.x before 10.6.41, and 10.7.x before 10.7.3 contains an unauthenticated denial of service vulnerability caused by uncontrolled recursion when validating query parameter and cookie values with a recursive regular expression engine before authentication in the WebAdmin and WebMail services. Attackers can send a single HTTP request with a query parameter or cookie value of a few thousand characters to exhaust the worker thread stack and crash the server process, taking down SMTP, IMAP, POP3, and web services repeatedly.	https://www.axigen.com/knowledgebase/Axigen-Server-Denial-of-Service-Vulnerability-via-Oversized-HTTP-Request-Parameters-CVE-Pending-_413.html https://www.axigen.com/updates/axigen-10.6.41 https://www.axigen.com/updates/axigen-10.7.3 https://www.vulncheck.com/advisories/axigen-mail-server-unauthenticated-dos-via-regex-recursion

https://nvd.nist.gov/vuln/detail/cve-2026-129494	7,5	CloudPaste 1.1.0	Insufficiently Protected Credentials	CloudPaste 1.1.0 through 1.9.1 contains an information disclosure vulnerability that allows unauthenticated attackers to obtain WebDAV storage credentials through the unauthenticated /api/proxy/link endpoint. Attackers who know a public share slug can retrieve the Basic Authorization header containing the WebDAV username and password, then read, modify, or delete files on the WebDAV server.	https://github.com/ling-drag0n/CloudPaste/blob/282ea1c7fbbcd4fab40527664bf7479fd5bb922d/backend/src/routes/proxyLinkRoutes.js#L139-L167 https://github.com/ling-drag0n/CloudPaste/blob/282ea1c7fbbcd4fab40527664bf7479fd5bb922d/backend/src/storage/drivers/webdav/WebDavStorageDriver.js#L800-L819 https://github.com/ling-drag0n/CloudPaste/issues/223 https://vul.yulun.ac.cn/20261115/cloudpaste/ https://www.vulncheck.com/advisories/cloudpaste-1.1.0-through-1.9.1-webdav-credential-disclosure-via-api-proxy-link
https://nvd.nist.gov/vuln/detail/cve-2026-129872	7,5	REBUILD 2.7.0	Improper Neutralization of Special Elements used in an SQL Command	REBUILD 2.7.0 through 4.5.4 contains an SQL injection vulnerability that allows low-privileged authenticated users to inject AjQL conditions through the plan parameter of /project/tasks/list. Attackers can use priority-* plans and the returned task count as a boolean oracle to recover a task creator's SHA-256 password hash and log in as that user, including the administrator.	https://github.com/getrebuild/rebuild/blob/741e3e50553665ef076596099ab04ff61ded8ddf/src/main/java/com/rebuild/web/project/ProjectTaskController.java#L127-L132 https://github.com/getrebuild/rebuild/blob/741e3e50553665ef076596099ab04ff61ded8ddf/src/main/java/com/rebuild/web/project/ProjectTaskController.java#L158-L168 https://vul.yulun.ac.cn/20261106/rebuild/ https://www.vulncheck.com/advisories/rebuild-2.7.0-through-4.5.4-sql-injection-via-plan-parameter-in-project-tasks-list
https://nvd.nist.gov/vuln/detail/cve-2026-130081	7,5	B3log Solo	Insertion of Sensitive Information Into Sent Data	B3log Solo through 4.4.0 contains an information disclosure vulnerability that allows unauthenticated attackers to obtain article view passwords by querying the public GET /articles API. The ArticleProcessor.getArticlesByPage handler leaves the articleViewPwd property in JSON responses, letting attackers read passwords for encrypted articles and access their protected content.	https://github.com/88250/solo/blob/v4.4.0/src/main/java/org/b3log/solo/processor/ArticleProcessor.java#L348-L369 https://github.com/88250/solo/blob/v4.4.0/src/main/java/org/b3log/solo/service/DataModelService.java#L785-L813 https://github.com/88250/solo/commit/46308431d479b61d4ac5cc768474efa140c23cc8 https://www.vulncheck.com/advisories/b3log-solo-through-4.4.0-article-view-password-disclosure-via-articles
https://nvd.nist.gov/vuln/detail/cve-2026-130374	7,5	AdminNeo	Improper Neutralization of Special Elements used in an SQL Command	AdminNeo before 5.9.1 contains an sql injection vulnerability that allows remote attackers to inject SQL by supplying crafted IN and NOT IN search values that process_length() passes unescaped. Attackers can send a logged-in user a cross-site GET link using a backslash-escaped apostrophe to run blind SQL with that user's database rights on PostgreSQL, SQLite, MS SQL,	https://github.com/adminneo-org/adminneo/releases/tag/v5.9.1 https://github.com/adminneo-org/adminneo/security/advisories/GHSA-r6wc-chqc-5wq3 https://www.vulncheck.com/advisories/adminneo-before-5.9.1-sql-injection-via-in-and-not-in-search-values

				Oracle, or MySQL in NO_BACKSLASH_ESCAPES mode.	
https://nvd.nist.gov/vuln/detail/cve-2026-129359	7,5	Linux Foundation Magma	Use of Hard-coded Password; Use of Hard-coded Credentials	A security flaw has been discovered in Linux Foundation Magma up to 1.9.0. The affected element is an unknown function of the file orc8r/lib/go/registry/interceptors.go. Performing a manipulation results in hard-coded credentials. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	https://vuldb.com/cve/CVE-2026-129359 https://vuldb.com/submit/1044005 https://vuldb.com/vuln/437422 https://vuldb.com/vuln/437422/cti https://www.linuxfoundation.org/
https://nvd.nist.gov/vuln/detail/cve-2026-116753	7,5	WordPress	Improper Neutralization of Input During Web Page Generation	The Multi Step for Contact Form 7 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'multipart field name (array key)' parameter in all versions up to, and including, 2.9.1 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 the target CF7 form to have the 'Save every step' option enabled and the Database for Contact Form 7 companion plugin to be active with its 'Expandable' table option enabled, both of which are disabled by default.	https://plugins.trac.wordpress.org/browser/cf7-multi-step/tags/2.9.1/inc/frontend/validation.php#L20 https://plugins.trac.wordpress.org/browser/cf7-multi-step/tags/2.9.1/inc/frontend/validation.php#L291 https://plugins.trac.wordpress.org/browser/cf7-multi-step/tags/2.9.1/inc/frontend/validation.php#L330 https://plugins.trac.wordpress.org/browser/cf7-multi-step/tags/2.9.2/inc/frontend/validation.php https://wordpress.org/plugins/cf7-multi-step/ https://www.wordfence.com/threat-intel/vulnerabilities/id/b9700627-97f2-4da1-a984-934062bd5014?source=cve
https://nvd.nist.gov/vuln/detail/cve-2026-129943	7,3	Prime CMS	Improper Neutralization of Special Elements used in an OS Command	Prime CMS (@primecms/core) through 0.4.0-beta.0 contains an OS command injection vulnerability in the updateSystem GraphQL mutation that allows authenticated administrators to execute shell commands via the package version string. Attackers can append shell metacharacters to the unvalidated version value, which is passed to child_process.exec() in yarn add or npm install commands, executing commands as the server process.	https://github.com/birkir/prime/blob/v0.3.4-beta.3/packages/prime-core/src/modules/internal/resolvers/PrimeResolver.ts#L110-L132 https://github.com/birkir/prime/blob/v0.3.4-beta.3/packages/prime-core/src/modules/internal/utils/updateNpmPackages.ts#L4-L15 https://github.com/birkir/prime/issues/549 https://www.vulncheck.com/advisories/prime-cms-through-0.4.0-beta.0-os-command-injection-via-updatesystem-mutation

https://nvd.nist.gov/vuln/detail/cve-2026-130351	7,2	Redis	Authorization Bypass Through User-Controlled Key	phpMyFAQ from 4.2.0-alpha before 4.2.0-RC.2 contains an authorization bypass vulnerability in the multisite Redis configuration store that is not tenant-scoped. As a result, tenant administrators can read and overwrite the master instance's effective configuration. Attackers can save configuration through /admin/api/configuration, optionally resetting storage.redisPrefix, to redirect master SMTP, set a known API token, or alter authentication settings.	https://github.com/thorsten/phpMyFAQ/releases/tag/4.2.0-RC.2 https://github.com/thorsten/phpMyFAQ/security/advisories/GHSA-6795-wmwp-422x https://www.vulncheck.com/advisories/phpmyfaq-4.2.0-alpha-before-4.2.0-rc.2-cross-tenant-configuration-overwrite-via-redis-store
https://nvd.nist.gov/vuln/detail/cve-2026-130375	7,2	AdminNeo	Unrestricted Upload of File with Dangerous Type	AdminNeo before 5.9.1 contains a remote code execution vulnerability that allows authenticated SQLite users to bypass the check_sqlite_name() extension guard using PDO_SQLite file: URI database names. Attackers can select the PDO driver with ext=pdo and submit names like file:/webroot/x.php?x=.db to create a .php file, then store PHP source as table data for code execution.	https://github.com/adminneo-org/adminneo/releases/tag/v5.9.1 https://github.com/adminneo-org/adminneo/security/advisories/GHSA-2gwx-67mg-hfr3 https://github.com/adminneo-org/adminneo/security/advisories/GHSA-r6xv-mvwg-hfrw https://www.vulncheck.com/advisories/adminneo-before-5.9.1-rce-via-sqlite-file-uri-database-name
https://nvd.nist.gov/vuln/detail/cve-2026-86676	7,2	Zyxel DX3300-T0	Improper Neutralization of Special Elements used in an OS Command	A post-authentication command injection vulnerability in the “Description” parameter of a CGI program in Zyxel DX3300-T0 firmware versions through 5.50(ABVY.8.3)C0 could allow an authenticated attacker with administrator privileges to execute OS commands by sending a crafted HTTP request.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-out-of-bounds-write-and-post-authentication-command-injection-vulnerabilities-in-certain-dsl-ethernet-cpe-fiber-onts-and-wireless-extenders-11-17-2026

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 Two Known Exploited Vulnerabilities to Catalog	▪ CVE-2026-114713 UnrealIRCd Improper Neutralization of Delimiters Vulnerability ▪ CVE-2026-123039 Check Point Multiple Products Incorrect Permission Assignment for Critical Resource Vulnerability	https://www.cisa.gov/news-events/alerts/2026/11/13/cisa-adds-two-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
Chase Software Bug Disrupts Banking Services as Customers Report Outages at Major US Banks	https://cybersecuritynews.com/chase-outage-disrupts-bank/
Meta Hit With €805 Million Fine Over Facebook's Unauthorized Access to Android Photo Galleries	https://cybersecuritynews.com/meta-hit-with-e805-million-fine/
Japan Reports Record 233 Cyber Incidents as 185 Million Personal Records Are Put at Risk	https://cybersecuritynews.com/233-cyber-incidents/
Microsoft Reveals How a Hidden Windows Bug Took Down Microsoft 365 Services Worldwide	https://cybersecuritynews.com/microsoft-outage-incident-report/
AWS Restores Services in US-EAST-1 After Hours-Long Outage Disrupts Cloud Operations	https://cybersecuritynews.com/aws-services-outage/
Claude Cracks 32-Year-Old Jeep ECU Using a $3 Arduino and Reverse Engineers Its Engine Computer	https://cybersecuritynews.com/claude-cracks-32-year-old-jeep-ecu/
Massive Microsoft 365 Outage Impacts Exchange Online, Teams, SharePoint, Copilot, and Defender XDR Users	https://cybersecuritynews.com/massive-microsoft-365-outage/
Microsoft 365 Massive Outage – Fixes Fail as Restored Servers Keep Going Unresponsive	https://cybersecuritynews.com/microsoft-365-massive-outage-fixes-fail-as-restored-servers-keep-going-unresponsive/
US Freezes $2.7 Billion Stolen by North Korean Hackers in Massive $6 Billion Binance Crypto Heist	https://cybersecuritynews.com/us-freezes-2-7-billion/

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 Infect 178 Major Websites via Optimizely to Steal Credit Cards and Target iPhones	https://cybersecuritynews.com/optimizely-websites-hijacked/
Australia's Supermarket Chain Coles Investigates Cyber Security Incident	https://cybersecuritynews.com/coles-investigates-cyber-security-incident/
Cursor Reveals How a Leaked Fireworks AI Key Led to a Backdoored Claude Code Extension	https://cybersecuritynews.com/cursor-data-breach/
Uber Confirms Data Breach – Hackers Stole Users' Personal Information	https://cybersecuritynews.com/uber-confirms-data-breach/
Hackers Use DeepSeek and GLM AI Agents to Breach 10 Organizations in Autonomous Cyberattacks	https://cybersecuritynews.com/deepseek-and-glm-ai-agents/

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
Researchers Reveal How Claude Code VS Code Extension Can Access Files Outside Trusted Workspaces	https://cybersecuritynews.com/claude-code-vs-code-extension/
NoisyTCP: 11-Year-Old Linux Kernel Flaw Lets Unauthenticated Attackers Crash Servers Remotely	https://cybersecuritynews.com/noisytcp-linux-kernel-vulnerability/
Researchers Find Six 0-Days Allowing Unauthorized Takeover of Supermarket Refrigeration Systems	https://cybersecuritynews.com/supermarket-refrigeration-systems-0-day/
CISA Warns of Check Point 0-Day Vulnerability Exploited to Gain Root Access	https://cybersecuritynews.com/check-point-0-day-vulnerability/

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
Microsoft Releases Out-of-band Update to Address Windows Licensing and Activation Errors	https://cybersecuritynews.com/microsoft-windows-licensing-error/
Apple Fixes iOS Flaw That Let Sandboxed Apps Secretly Record Microphone Audio Without Permission	https://cybersecuritynews.com/apple-fixes-ios-flaw/
Tor Releases Emergency Security Update as Ongoing DDoS Attack Overwhelms Network Relays	https://cybersecuritynews.com/tor-ddos-attack/
Citrix Patches 28 Security Vulnerabilities in NetScaler, Including a Critical Flaw in Default Installations	https://cybersecuritynews.com/citrix-patches-netscaler-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
Hackers Use AI-Powered Marketplace to Find Infected Computers With Corporate VPN and Cloud Access	https://cybersecuritynews.com/hackers-use-ai-powered-marketplace/
Retadup USB Worm Returns After 7 Years, Spreading CoffeeLoader Malware to Windows Systems	https://cybersecuritynews.com/retadup-usb-worm-returns/
Cisco Talos Reveals How Hackers Use ARTEX, PentAGI, and HexStrike AI to Automate Cyberattacks	https://cybersecuritynews.com/hackers-use-artex/
Google Reveals How Hackers Are Using AI Agents to Automate Real-World Cyberattacks	https://cybersecuritynews.com/fully-automated-ai-attacks/
Mustang Panda-Linked Hackers Deploy LOTUSLITE V2 Through Malicious Zoho WorkDrive Downloads	https://cybersecuritynews.com/mustang-panda-linked-hackers/
Nine Underground Listings Reveal How Hackers Sell Access to Enterprise VPNs, Cloud, and CI/CD Systems	https://cybersecuritynews.com/nine-underground-listings/
Hackers Use ARTEX AI Agents to Automate Network Intrusions and Gain Privileged Access in Under 3 Hour	https://cybersecuritynews.com/hackers-use-artex-ai-agents-2/

Σύντομη περιγραφή / Τίτλος	URL
Hackers Use Falcon C2 to Hijack Government Browsers and Steal Passwords, Emails, and Session Cookies	https://cybersecuritynews.com/hackers-use-falcon-c2/
BlackNevas Ransomware Wipes VMware ESXi Infrastructure and Backups Without Exploiting Any Flaws	https://cybersecuritynews.com/blacknevas-ransomware/
FBI Reveals How Hackers Hid Malware in Video Games to Steal $220,000 From Cryptocurrency Wallets	https://cybersecuritynews.com/fbi-cryptocurrency-theft-warning/
FBI Reveals How Hackers Use ARTEX AI Agents to Gain Privileged Access in Under Three Hours	https://cybersecuritynews.com/fbi-reveals-hackers-artex-ai-usage/
Microsoft Warns of Active Password Stealing Attack Exploiting the Microsoft 365 Service Disruption	https://cybersecuritynews.com/active-password-stealing-attack-microsoft-365/
New TypoPrompting Attacks Turn Mistyped AI Website Addresses Into Malware Installation Traps	https://cybersecuritynews.com/new-typoprompting-attacks/
Hackers Use SANSAR Linux Malware to Hide Crypto Mining by Faking 0% GPU Usage	https://cybersecuritynews.com/hackers-use-sansar-linux-malware/
Hackers Use 2,700 Passwords to Break Into Microsoft SQL Servers and Deploy Remote Access Malware	https://cybersecuritynews.com/break-into-microsoft-sql-servers/
Hackers Use Fake Purchase Order Emails to Deliver XLoader Malware Through Malicious Word Documents	https://cybersecuritynews.com/fake-purchase-order-emails/
Hackers Use Windows Named Pipes and SMB to Spread Malware Across Isolated Government Networks	https://cybersecuritynews.com/windows-named-pipes-and-smb/
Beast Ransomware Uses Hidden ‘666’ Control Panel to Encrypt Windows Systems and Network Shares	https://cybersecuritynews.com/beast-ransomware/
ArcticRAT Android Malware Uses Hidden VNC to Control Smartphones While Showing Victims a Black Screen	https://cybersecuritynews.com/arcticrat-android-malware/

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
Apple Reveals How Secure Exclaves Prevent Hidden Camera and Microphone Access on iPhones	https://cybersecuritynews.com/apple-reveals-secure-exclaves/
New OWASP Top 10 Exposes Hidden Security Weaknesses in Neocloud and AI Infrastructure	https://cybersecuritynews.com/owasp-top-10-incubator/
Claude Gets VirusTotal Threat Intelligence Capabilities for AI-Assisted Malware and URL Analysis	https://cybersecuritynews.com/claude-gets-virustotal-threat-intelligence/
Top 10 Best Cyber Asset Attack Surface Management (CAASM) Tools in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-caasm-tools/
Top 10 Best Attack Surface Management (ASM/EASM) Tools in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-attack-surface-management/
Top 10 Best Continuous Threat Exposure Management (CTEM) Platforms in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-ctem-platforms/
Top 10 Best Risk-Based Vulnerability Management Tools in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-rbvm-tools/
Top 10 Best Cloud Vulnerability Management Tools in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-cloud-vulnerability-management/
Top 10 Best Network Vulnerability Scanners in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-network-vulnerability-scanners/
Top 10 Best Web Application Vulnerability Scanners in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-web-app-scanners/
Top 10 Best Vulnerability Scanners in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-vulnerability-scanners/
Top 10 Best Vulnerability Management Tools in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-vulnerability-management-tools/
Top 10 Best AI Governance (AI TRiSM) Platforms in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-ai-governance-platforms/

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/