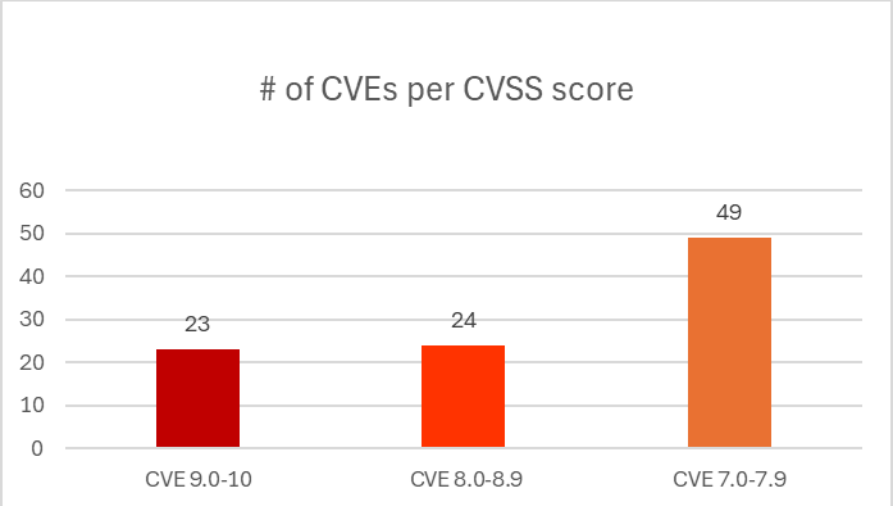
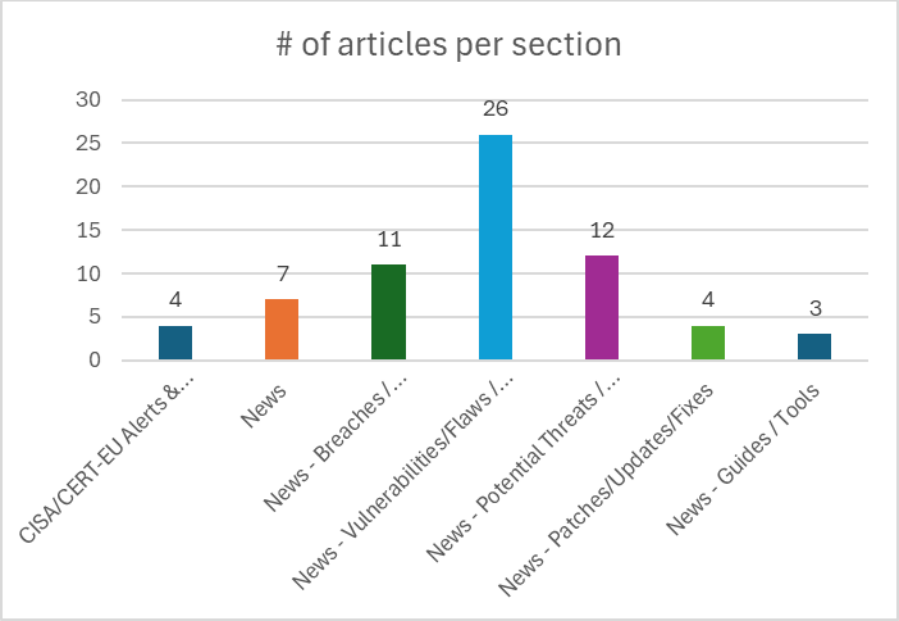


Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 21/11/2026 - 24/11/2026





Contents

Common Vulnerabilities and Exposures (CVEs) 3
CISA/CERT-EU Alerts & Advisories 21
News 22
Breaches / Compromised / Hacked 23
Vulnerabilities / Flaws / Zero-day 24
Patches / Updates / Fixes 26
Potential threats / Threat intelligence 26
Guides / Tools 27
References 28
Annex – Websites with vendor specific vulnerabilities 29

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	Vendor	Τύπος Ευπάθειας	Περιγραφή (Description)	References
https://nvd.nist.gov/vuln/detail/cve-2026-133993	10,0	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer; Stack-based Buffer Overflow	A security flaw has been discovered in D-Link DIR-600L 2.17b02. This affects the function FUN_0040efb0 of the file gena.cgi of the component GENA Subscription Handler. Performing a manipulation of the argument service results in stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks.	https://github.com/ruanyi101/router-firmware-security-advisories/blob/main/router-firmware-GitHub-advisories/related-findings/D-Link-DIR-600L-gena-cgi-stack-overflow-review.md https://vuldb.com/cve/CVE-2026-133993 https://vuldb.com/submit/1052046 https://vuldb.com/vuln/441598 https://vuldb.com/vuln/441598/cti https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/cve-2026-62841	10,0	Microsoft	Improper Authentication	Improper authentication in Azure Event Grid allows an unauthorized attacker to elevate privileges over a network.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62841
https://nvd.nist.gov/vuln/detail/cve-2026-130169	10,0	Significant-Gravitas	Improper Authentication; Use of Insufficiently Random Values; Use of Hard-coded Credentials	AutoGPT is a workflow automation platform for creating, deploying, and managing continuous artificial intelligence agents. In versions 0.6.26 through 0.7.4, AutoGPT Platform ships a publicly known, hardcoded default JWT verification key in backend/.env.default and autogpt_platform/.env.default. Because HS256 is symmetric, anyone who knows the secret can forge valid JWTs for any user or for the admin role, bypassing authentication and authorization without user interaction. This issue is fixed in version 0.8.0.	https://github.com/Significant-Gravitas/AutoGPT/releases/tag/autogpt-platform-beta-v0.8.0 https://github.com/Significant-Gravitas/AutoGPT/security/advisories/GHSA-24q6-6h89-f9p7
https://nvd.nist.gov/vuln/detail/cve-2026-134882	10,0	TOTOLINK	Improper Neutralization of Special Elements used in a Command; Improper Neutralization of Special Elements used in an OS Command	A weakness has been identified in TOTOLINK A7100RU 7.4cu.2313_B20191024. This issue affects the function exportOvpn of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. This manipulation of the argument Username causes os command injection. The attack is possible to be carried out remotely.	https://vuldb.com/cve/CVE-2026-134882 https://vuldb.com/submit/1054781 https://vuldb.com/vuln/442238 https://vuldb.com/vuln/442238/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/cve-	9,9	Dell	Improper Neutralization of Argument Delimiters in a Command	Dell Enterprise Sonic Distribution, versions prior to 4.6.1, contains an Argument Injection vulnerability. A low privileged remote attacker could potentially exploit this vulnerability, leading to arbitrary command execution and unauthorized access to filesystem resources.	https://www.dell.com/support/kbdoc/en-us/000535884/dsa-2026-451-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities

2026-103782					
https://nvd.nist.gov/vuln/detail/cve-2026-50691	9,9	Microsoft	Improper Authorization	Improper authorization in M365 Copilot allows an authorized attacker to elevate privileges over a network.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50691
https://nvd.nist.gov/vuln/detail/cve-2026-70193	9,9	Microsoft	Improper Limitation of a Pathname to a Restricted Directory	Improper limitation of a pathname to a restricted directory ('path traversal') in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70193
https://nvd.nist.gov/vuln/detail/cve-2026-114021	9,8	Apple	Out-of-bounds Write	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Golden Gate 27.2, macOS Sequoia 15.8.2, macOS Tahoe 26.7.2. Connecting to a malicious NFS server may lead to kernel memory corruption.	https://support.apple.com/en-us/149521 https://support.apple.com/en-us/149522 https://support.apple.com/en-us/149523
https://nvd.nist.gov/vuln/detail/cve-2026-114022	9,8	Apple	Out-of-bounds Write	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.8.2, macOS Tahoe 26.7.2. An app may be able to cause unexpected system termination.	https://support.apple.com/en-us/149522 https://support.apple.com/en-us/149523
https://nvd.nist.gov/vuln/detail/cve-2026-114025	9,8	Apple	Out-of-bounds Write	An out-of-bounds write was addressed with improved input validation. This issue is fixed in iOS 26.7.2 and iPadOS 26.7.2, iOS 27.2 and iPadOS 27.2, macOS Golden Gate 27.2, macOS Sequoia 15.8.2, macOS Tahoe 26.7.2, tvOS 27.2. A user may be able to cause unexpected app termination or arbitrary code execution.	https://support.apple.com/en-us/149227 https://support.apple.com/en-us/149230 https://support.apple.com/en-us/149521 https://support.apple.com/en-us/149522 https://support.apple.com/en-us/149523 https://support.apple.com/en-us/149524
https://nvd.nist.gov/vuln/detail/cve-2026-132475	9,8	Apple	Out-of-bounds Write	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Golden Gate 27.2. An app may be able to cause unexpected system termination or corrupt kernel memory.	https://support.apple.com/en-us/149521
https://nvd.nist.gov/vuln/detail/cve-2026-135208	9,8	kerberos-io	Use of Default Cryptographic Key	Kerberos Agent before 3.14.4 contains an authentication bypass vulnerability that allows unauthenticated attackers to forge administrator tokens because JWTMiddleWare() falls back to the hard-coded key TOBECHANGED. Attackers can sign HS256 tokens with arbitrary username and role claims to access /api and /config routes, exposing RTSP, ONVIF, Hub and encryption keys, rewriting configuration, and stopping the camera.	https://github.com/kerberos-io/agent/blob/v3.14.1/machinery/src/routers/http/jwt_middleware.go#L17-L28 https://github.com/kerberos-io/agent/commit/c0baade8fd6e21ed1b9a834d9ae6b4eaaa67b3b6 https://github.com/kerberos-

					io/agent/pull/361 https://github.com/kerberos-io/agent/releases/tag/v3.14.4 https://github.com/kerberos-io/agent/security/advisories/GHSA-3c52-7fc8-c39j https://www.vulncheck.com/advisories/kerberos-agent-before-3.14.4-authentication-bypass-via-hard-coded-jwt-signing-key
https://nvd.nist.gov/vuln/detail/cve-2026-120382	9,8	Synology	Improper Neutralization of Argument Delimiters in a Command	An improper neutralization of argument delimiters in a command vulnerability in the OAuth API in Synology DiskStation Manager (DSM) before 7.1.1-42962-10, 7.2.1-69057-14, 7.2.2-72806-11, 7.3.2-86009-6, and 7.4.1-90080-2 allows remote attackers to read or write arbitrary files and conduct denial-of-service attacks.	https://www.synology.com/en-global/security/advisory/Synology_SA_26_21
https://nvd.nist.gov/vuln/detail/cve-2026-103788	9,6	Dell	Improper Neutralization of Special Elements used in an OS Command	Dell Enterprise Sonic Distribution, versions prior to 4.6.1, contains an OS Command Injection vulnerability. An unauthenticated adjacent network attacker could potentially exploit this vulnerability, leading to arbitrary command execution. This vulnerability is considered critical as it may allow unauthenticated command execution.	https://www.dell.com/support/kbdoc/en-us/000535884/dsa-2026-451-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities
https://nvd.nist.gov/vuln/detail/cve-2026-134401	9,6	Google	Improper Input Validation	Improper input validation in Variations in Google Chrome prior to 158.0.8127.88 allowed a remote attacker to potentially execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: Critical)	https://chromereleases.googleblog.com/2026/11/stable-channel-update-for-desktop_01734282054.html https://issues.chromium.org/issues/554051967
https://nvd.nist.gov/vuln/detail/cve-2026-109480	9,6	Microsoft	Not specified	Server-side request forgery in Profile Data Roaming Service (PDRS) allows an authorized attacker to elevate privileges over a network.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-109480
https://nvd.nist.gov/vuln/detail/cve-2026-118285	9,6	Microsoft	Server-Side Request Forgery	Server-side request forgery in Azure Machine Learning allows an authorized attacker to elevate privileges over a network.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-118285
https://nvd.nist.gov/vuln/detail/cve-2026-70305	9,6	Microsoft	Improper Neutralization of Input During Web Page Generation	Improper neutralization of input during web page generation ('cross-site scripting') in Azure Portal allows an unauthorized attacker to perform spoofing over a network.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70305

https://nvd.nist.gov/vuln/detail/cve-2026-109490	9,3	Microsoft	Improper Neutralization of Input During Web Page Generation	Improper neutralization of input during web page generation ('cross-site scripting') in Authentication Methods Portal Extension allows an unauthorized attacker to elevate privileges over a network.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-109490
https://nvd.nist.gov/vuln/detail/cve-2026-113824	9,1	Microsoft	Authorization Bypass Through User-Controlled Key	Authorization bypass through user-controlled key in Microsoft Clarity allows an unauthorized attacker to elevate privileges over a network.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-113824
https://nvd.nist.gov/vuln/detail/cve-2026-118286	9,1	Microsoft	Improper Access Control	Improper access control in Azure Site Recovery allows an unauthorized attacker to elevate privileges over a network.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-118286
https://nvd.nist.gov/vuln/detail/cve-2026-69899	9,1	Microsoft	Authentication Bypass by Spoofing	Authentication bypass by spoofing in Azure DevTest Labs allows an unauthorized attacker to perform spoofing over a network.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69899
https://nvd.nist.gov/vuln/detail/cve-2026-135429	9,1	TabbycatDebate	Incorrect Authorization	Tabbycat 2.9.0 through 2.12.1 contains an incorrect authorization vulnerability in TournamentViewSet that allows unauthenticated attackers to gain write access because PerTournamentPermissionRequired returns True for views lacking a tournament attribute. Attackers can send POST, PUT, PATCH or DELETE requests to /api/v1/tournaments to create, modify or delete tournaments, cascading deletion to teams and speakers.	https://github.com/TabbycatDebate/tabbycat/blob/v2.12.1/tabbycat/api/permissions.py#L71-L75 https://github.com/TabbycatDebate/tabbycat/commit/b7f0746ba9cb5a23f94ac169dbe5b68a5fbd1ab2 https://github.com/TabbycatDebate/tabbycat/issues/3047 https://www.vulncheck.com/advisories/tabbycat-2.9.0-through-2.12.1-unauthenticated-tournament-modification-via-rest-api
https://nvd.nist.gov/vuln/detail/cve-2026-86312	8,8	Apache Software Foundation	Unintended Proxy or Intermediary; Exposed Dangerous Method or Function	Under some configurations a request to the ping endpoint could carry out more than a simple health check. In deployments that rely on Solr's rule-based authorization, a client granted only the low-privilege health permission could thereby trigger behavior that should require higher privileges; where the shipped security.json template leaves the health permission unauthenticated, no credentials are required at all. This issue affects Apache Solr from 9.0.0 through the releases preceding the fixed versions. Users are recommended to upgrade to version 9.11.0 or 10.1.0, which resolve the issue. You are affected if you run an affected version and allow the /admin/ping endpoint to be reached with only the health permission. This includes the default sample security configuration installed by the bin/solr CLI, where that endpoint is unauthenticated. Users who cannot upgrade immediately	https://github.com/apache/solr/pull/4890 https://lists.apache.org/thread/23vlsohrl7vcckysqp9d094yplt4pjcv http://www.openwall.com/lists/oss-security/2026/11/23/9

				should restrict access to the /admin/ping endpoint in their authorization configuration — for example by requiring a trusted role for that path — and ensure Solr is not reachable from untrusted clients or networks, as recommended for all Solr deployments.	
https://nvd.nist.gov/vuln/detail/cve-2026-114023	8,8	Apple	Improper Limitation of a Pathname to a Restricted Directory	A path handling issue was addressed with improved validation. This issue is fixed in macOS Golden Gate 27.2, macOS Sequoia 15.8.2, macOS Tahoe 26.7.2. Processing web content may lead to arbitrary code execution.	https://support.apple.com/en-us/149521 https://support.apple.com/en-us/149522 https://support.apple.com/en-us/149523
https://nvd.nist.gov/vuln/detail/cve-2026-134359	8,8	AzuraCast	Improper Neutralization of Escape, Meta, or Control Sequences	AzuraCast before 0.24.1 fails to escape backslashes in Liquidsoap annotation values, allowing media managers to break out of quoted annotation strings. Attackers can set a crafted ID3 title ending in a backslash to inject a process: protocol URI, achieving OS command execution in the Liquidsoap container during playback.	https://github.com/AzuraCast/AzuraCast/security/advisories/GHSA-mf65-hj88-hvrw https://www.vulncheck.com/advisories/azuracast-before-0.24.1-os-command-injection-via-liquidsoap-annotation-values
https://nvd.nist.gov/vuln/detail/cve-2026-95793	8,8	Hewlett Packard Enterprise	Not specified	An arbitrary remote code execution vulnerability exists in HPE Morpheus Manager.	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbvs05182en_us&docLocale=en_US
https://nvd.nist.gov/vuln/detail/cve-2026-129794	8,8	RT-Labs AB	Out-of-bounds Write	The EoE fragment reassembly code uses a frame size from the wire as the bound for memcpy into the application receive buffer, without checking that the declared size fits in the actual buffer. A master can write up to 2016 bytes into a buffer the application may have sized much smaller.	https://docs.rt-labs.com/security/advisories/rrtl-261119-01.html
https://nvd.nist.gov/vuln/detail/cve-2026-129796	8,8	RT-Labs AB	Integer Underflow (Wrap or Wrapa-round); Out-of-bounds Write	The CoE SDO download handler for flexible-length objects (VISIBLE_STRING, OCTET_STRING, and similar) does not check that the master-declared transfer size fits within the object before writing. Two distinct writes are affected: the VISIBLE_STRING zero-padding memset and the first-frame copy into the object buffer.	https://docs.rt-labs.com/security/advisories/rrtl-261119-01.html
https://nvd.nist.gov/vuln/detail/cve-2026-129797	8,8	RT-Labs AB	NULL Pointer Dereference	SDO_downloadsegment is called whenever a mailbox frame carries the DOWNLOADSEGREQ command byte, regardless of whether a segmented download is actually in progress. ESCvar.data, which the handler writes through, is NULL until a segmented transfer is started. A master can send a DOWNLOADSEGREQ at any time and write through a NULL or stale pointer.	https://docs.rt-labs.com/security/advisories/rrtl-261119-01.html
https://nvd.nist.gov/vuln/detail/cve-2026-129798	8,8	RT-Labs AB	Out-of-bounds Write	The CoE SDO segmented download handler advances a write pointer by each incoming segment's size but does not track how many bytes have been written in total. A master can keep sending non-last segments until the pointer has walked past the end of the object buffer or the complete-access staging buffer.	https://docs.rt-labs.com/security/advisories/rrtl-261119-01.html

https://nvd.nist.gov/vuln/detail/cve-2026-129811	8,8	RT-Labs AB	Out-of-bounds Write	The PDO mapping bit lengths stored in the mapping objects are writable by the master via SDO. sizeOfPDO summed them without checking the total against the size of the rxpdo[] or txpdo[] process data buffers. A master can craft a mapping whose total bit count exceeds those buffers, causing COE_pdoPack and COE_pdoUnpack to write past their ends during each process data cycle after the PREOP to SAFEOP transition.	https://docs.rt-labs.com/security/advisories/rrtl-261119-01.html
https://nvd.nist.gov/vuln/detail/cve-2026-123886	8,8	Spring	Not specified	Spring Data Elasticsearch replaces positional placeholders in string-based @Query methods with the method arguments before it evaluates SpEL expressions in the resulting query string. As a result, an argument that contains a SpEL expression is evaluated as part of the query, even if the declared query does not use SpEL. An application is affected if it passes untrusted input as an argument to a repository query method that declares a @Query with positional placeholders. In that case, a remote attacker can execute arbitrary code in the application, and repeated requests can exhaust memory through the unbounded expression cache.	https://spring.io/security/cve-2026-123886
https://nvd.nist.gov/vuln/detail/cve-2026-120747	8,8	Tanium	Improper Neutralization of Special Elements used in an OS Command	Tanium addressed a command injection vulnerability in Comply.	https://security.tanium.com/TAN-2026-140
https://nvd.nist.gov/vuln/detail/cve-2026-133985	8,8	TRENDnet	Improper Restriction of Operations within the Bounds of a Memory Buffer; Out-of-bounds Read	A flaw has been found in TRENDnet TEW-657BRM 1.00.1. Affected by this issue is some unknown functionality of the file /usr/sbin/restore_config.cgi. Executing a manipulation can lead to out-of-bounds read. The attack may be launched remotely. The exploit has been published 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-restore_config-cgi.md https://vuldb.com/cve/CVE-2026-133985 https://vuldb.com/submit/1052043 https://vuldb.com/vuln/441575 https://vuldb.com/vuln/441575/cti
https://nvd.nist.gov/vuln/detail/cve-2026-69437	8,6	Microsoft	Missing Authorization	Missing authorization in Azure AI Foundry allows an unauthorized attacker to disclose information over a network.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69437
https://nvd.nist.gov/vuln/detail/cve-2026-81962	8,6	Microsoft	Missing Authorization	Incorrect authorization in Azure Machine Learning allows an unauthorized attacker to disclose information over a network.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81962
https://nvd.nist.gov/vuln/detail/cve-	8,4	NLnet Labs	Allocation of Resources Without Limits or Throttling	An rsync server can send diagnostic data to the client which is mirrored to stdout and collected by Routinator line by line. If an excessive amount of data is sent without a line break, Routinator will eventually run out of memory and crash.	https://www.nlnetlabs.nl/downloads/krill/CVE-2026-119068.txt

2026-119068					
https://nvd.nist.gov/vuln/detail/cve-2026-119069	8,4	NLnet Labs	Improper Handling of Structural Elements	When rejecting a publication point midway during processing amd falling back to the stored version of the publication point, Routinator will keep the data it had processed for the publication point so far rather than dropping it.	https://www.nlnetlabs.nl/downloads/krill/CVE-2026-119069.txt
https://nvd.nist.gov/vuln/detail/cve-2026-65817	8,3	Microsoft	Improper Neutralization of Special Elements used in an OS Command	Improper neutralization of special elements used in an os command ('os command injection') in Azure Managed Instance for Apache Cassandra allows an unauthorized attacker to execute code over an adjacent network.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65817
https://nvd.nist.gov/vuln/detail/cve-2026-101218	8,2	Dell	Improper Neutralization of Special Elements used in an OS Command	Dell Enterprise Sonic Distribution, versions prior to 4.6.1, contains an OS Command Injection vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution.	https://www.dell.com/support/kbdoc/en-us/000535884/dsa-2026-451-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities
https://nvd.nist.gov/vuln/detail/cve-2026-103783	8,2	Dell	Improper Neutralization of Special Elements used in an OS Command	Dell Enterprise Sonic Distribution, versions prior to 4.6.1, contains an OS Command Injection vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution.	https://www.dell.com/support/kbdoc/en-us/000535884/dsa-2026-451-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities
https://nvd.nist.gov/vuln/detail/cve-2026-135736	8,1	FFmpeg	Out-of-bounds Write	FFmpeg 4.4 before 9.1 contains a heap out-of-bounds read and write vulnerability in libavfilter/vf_deband.c that allows attackers to corrupt heap memory by sending a runtime coupling command. Attackers can send a 'deband coupling 1' command via sendcmd or an unauthenticated zmq filter, making chroma planes be processed at luma dimensions to crash the process or potentially execute code.	https://code.ffmpeg.org/FFmpeg/FFmpeg/pulls/26081 https://github.com/FFmpeg/FFmpeg https://github.com/FFmpeg/FFmpeg/blob/n9.0.2/libavfilter/vf_deband.c#L212 https://github.com/FFmpeg/FFmpeg/commit/24ad423d908cd595c983b6c503ddb0ee94901ba2 https://www.vulncheck.com/advisories/ffmpeg-4.4-before-9.1-heap-out-of-bounds-write-via-deband-filter-coupling-command
https://nvd.nist.gov/vuln/detail/cve-2026-135743	8,1	FFmpeg	Out-of-bounds Write	FFmpeg 4.3 before 9.1 contains a heap out-of-bounds read and write vulnerability in the dynaudnorm filter because cqueue_resize() miscalculates gain history queue element counts when gausssize changes at runtime. Attackers can send gausssize commands via asendcmd scripts or an unauthenticated azmq filter to corrupt heap memory, crashing the process or potentially executing code.	https://code.ffmpeg.org/FFmpeg/FFmpeg/pulls/26081 https://github.com/FFmpeg/FFmpeg https://github.com/FFmpeg/FFmpeg/blob/n9.0.2/libavfilter/af_dynaudnorm.c#L261 https://github.com/FFmpeg/FFmpeg/commit/3dd257f99b5cdc1bf38e1cadff1e34ec559c

					7b7c https://www.vulncheck.com/advisories/ffmpeg-4.3-before-9.1-heap-out-of-bounds-read-write-via-dynaudnorm-filter
https://nvd.nist.gov/vuln/detail/cve-2026-134841	8,1	pgjdbc	Improper Neutralization of Special Elements used in an SQL Command	pgjdbc, the PostgreSQL JDBC Driver, misreads some quoted text in its query parser. A `}` inside a literal ends a JDBC escape such as `{ts}`, and the rest of the literal is translated as SQL. A dollar quote whose tag has a non-ASCII symbol or space is not recognized. An `E'` string with a doubled quote is scanned as a standard string. `{fn right}` and `{fn timestampdiff}` with a negative argument produce a `--` comment. In each case text that the application quoted correctly can run as SQL with the privileges of the application's database role. All versions before 42.7.15 are affected, and 42.7.15 fixes the problem.	https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-4743-5rfh-f7mp
https://nvd.nist.gov/vuln/detail/cve-2026-134842	8,1	pgjdbc	Improper Neutralization of Special Elements used in an SQL Command	pgjdbc, the PostgreSQL JDBC Driver, can quote a string parameter for the wrong value of standard_conforming_strings when preferQueryMode=simple is set. A statement, trigger or configuration reload can turn the setting off during a session. A parameter value with a backslash and a quote then ends the literal, and the rest of the value runs as SQL. Before 42.7.6 any session with the setting off was affected. The statement cache can also reuse a parse made under the other setting. With allowEncodingChanges=true and the EUC_JP or SJIS client encoding, the yen sign acts as a backslash. All versions before 42.7.15 are affected, and 42.7.15 fixes the problem.	https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-6rxc-3r4p-gpff
https://nvd.nist.gov/vuln/detail/cve-2026-135055	8,0	Red Hat	Out-of-bounds Read	A flaw was found in the GLib DMA-BUF path of WebKitGTK. The UIProcess trusted fds.size() as the DMA-BUF plane count when handling AcceleratedBackingStore::DidCreateDMABufBuffer and copied offsets and strides without verifying that those vectors had the same length. A compromised WebProcess can send mismatched vector lengths, causing an out-of-bounds read in the privileged UIProcess. This can disclose UIProcess memory and crash the UIProcess, and may be used as part of a Web Content sandbox-escape chain.	https://access.redhat.com/security/cve/CVE-2026-135055 https://bugs.webkit.org/show_bug.cgi?id=329646 https://bugs.webkit.org/show_bug.cgi?id=330367 https://bugzilla.redhat.com/show_bug.cgi?id=2581773 https://github.com/WebKit/WebKit/commit/7f5f4ad7fe55 https://webkitgtk.org/ https://wpewebkit.org/release/wpewebkit-2.54.3.html
https://nvd.nist.gov/vuln/detail/cve-2026-112603	7,8	Apple	Improper Privilege Management	A logic issue was addressed with improved checks. This issue is fixed in Xcode 27.2. An app may be able to gain root privileges.	https://support.apple.com/en-us/149589
https://nvd.nist.gov/vuln/detail/cve-2026-113953	7,8	Apple	Integer Overflow or Wraparound	An integer overflow was addressed with improved input validation. This issue is fixed in iOS 27.2 and iPadOS 27.2, macOS Golden Gate 27.2, macOS Sequoia 15.8.2, macOS Tahoe 26.7.2, tvOS 27.2, visionOS 27.2. Processing a maliciously crafted USD file may lead to unexpected app termination.	https://support.apple.com/en-us/149230 https://support.apple.com/en-us/149521 https://support.apple.com/en-us/149522 https://support.apple.com/en-us/149523 https://support.apple.com/en-us/149524 https://support.apple.com/en-us/149526
https://nvd.nist.gov	7,8	Apple	Use After Free	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 27.2 and iPadOS 27.2. Processing a maliciously crafted file may lead to unexpected app termination.	https://support.apple.com/en-us/149230

/vuln/detail/cve-2026-113954					
https://nvd.nist.gov/vuln/detail/cve-2026-132856	7,8	checkpoint	Improper Link Resolution Before File Access; Improper Verification of Cryptographic Signature	A vulnerability was discovered in the ZoneAlarm client for Windows that allows a low-privileged local user to run code with SYSTEM privileges. An attacker must first be able to run code on the target system as a local user.	https://support.checkpoint.com/results/sk/sk1000415
https://nvd.nist.gov/vuln/detail/cve-2026-134793	7,8	electerm	Improper Neutralization of Special Elements used in an OS Command	Electerm before 5.9.0 on Windows contains an OS command injection vulnerability that allows attackers to execute PowerShell code via crafted file or folder names containing Unicode quote characters. Attackers can deliver names containing U+2019 through archives, WSL distributions, or SMB shares, which break out of getFolderSizeWin() and calcLocal() quoting when victims request folder sizes, executing code as the electerm user.	https://github.com/electerm/electerm/blob/v5.8.0/src/app/lib/fs.js#L106-L115 https://github.com/electerm/electerm/blob/v5.8.0/src/client/components/sftp/file-info-modal.jsx#L183-L192 https://github.com/electerm/electerm/commit/488b112d10dc21545f18284d4eb52db6dafb7f31 https://github.com/electerm/electerm/pull/4710 https://github.com/electerm/electerm/releases/tag/v5.9.0 https://github.com/electerm/electerm/security/advisories/GHSA-h4v2-5hq4-wc2g https://www.vulncheck.com/advisories/electerm-before-5.9.0-os-command-injection-via-unicode-quotes-in-powershell
https://nvd.nist.gov/vuln/detail/cve-2026-135722	7,8	FFmpeg	Heap-based Buffer Overflow	FFmpeg before 9.1 contains a heap-based buffer overflow vulnerability in peak_init_writer() and wav_write_packet() in libavformat/wavenc.c that allows attackers to corrupt heap memory by supplying audio with zero channels. Attackers can provide a crafted PCM stream declaring no channels for WAV output with peak envelope enabled, causing out-of-bounds writes past peak_maxpos and peak_maxneg arrays, crashes, and potential code execution.	https://code.ffmpeg.org/FFmpeg/FFmpeg/pulls/24932 https://github.com/FFmpeg/FFmpeg https://github.com/FFmpeg/FFmpeg/blob/n9.0.2/libavformat/wavenc.c#L391 https://github.com/FFmpeg/FFmpeg/commit/0b1c279b62af82e422e3fc21ba6cc2fc3154dc76 https://www.vulncheck.com/advisories/ffmpeg-before-9.1-heap-buffer-overflow-via-wav-muxer-peak-envelope-writer
https://nvd.nist.gov/vuln/detail/cve-2026-135725	7,8	FFmpeg	Stack-based Buffer Overflow	FFmpeg before 9.1 contains a stack-based buffer overflow vulnerability in ff_rtmp_packet_write() in libavformat/rtmppkt.c that allows malicious RTMP servers to overflow a 16-byte header buffer. Attackers can send a Set Chunk Size packet on a high channel id with an extended timestamp, which handle_chunk_size() echoes back, corrupting the publishing client's stack.	https://code.ffmpeg.org/FFmpeg/FFmpeg/pulls/24916 https://github.com/FFmpeg/FFmpeg https://github.com/FFmpeg/FFmpeg/blob/n9.0.2/libavformat/rtmppkt.c#L317 https://github.com/FFmpeg/FFmpeg/commit/041098a1a3bee481a1c8e905257ba04dad

					0c60a1 https://www.vulncheck.com/adviso-ries/ffmpeg-before-9.1-stack-based-buffer-overflow-via-ff-rtmp-packet-write
https://nvd.nist.gov/vuln/de-tail/cve-2026-135734	7,8	FFmpeg	Out-of-bounds Write	FFmpeg before 9.1 contains a heap out-of-bounds write vulnerability in the deflicker filter that lets attackers corrupt heap memory via unclamped high bit depth luma samples. Attackers can supply crafted video whose luma values exceed the nominal depth, making calc_avgy16() increment counters past the histogram allocation, causing crashes or possibly code execution.	https://code.ffmpeg.org/FFmpeg/FFmpeg/pulls/26121 https://github.com/FFmpeg/FFmpeg https://github.com/FFmpeg/FFmpeg/blob/n9.0.2/libavfilter/vf_deflicker.c#L193 https://github.com/FFmpeg/FFmpeg/com-mit/fa10042f748f20fad0cc0ee8fdcebe96b76603af https://www.vulncheck.com/adviso-ries/ffmpeg-before-9.1-heap-out-of-bounds-write-via-deflicker-filter-histogram
https://nvd.nist.gov/vuln/de-tail/cve-2026-135737		FFmpeg	Out-of-bounds Write	FFmpeg before 9.1 contains a heap out-of-bounds write and read vulnerability in the tmidequalizer filter that allows attackers to corrupt memory by supplying high bit depth samples exceeding the nominal maximum. Attackers can craft planar 9, 10, 12 or 14 bit video so compute_histogram16() and apply_contrast_change16() index unclamped samples, crashing applications, corrupting the heap, and leaking heap contents.	https://code.ffmpeg.org/FFmpeg/FFmpeg/pulls/26121 https://github.com/FFmpeg/FFmpeg https://github.com/FFmpeg/FFmpeg/blob/n9.0.2/libavfilter/vf_tmidequalizer.c#L312 https://github.com/FFmpeg/FFmpeg/com-mit/1e1e424bd8d7a50a8213da1e95a92f524e9b801d https://www.vulncheck.com/adviso-ries/ffmpeg-before-9.1-heap-out-of-bounds-write-via-tmidequalizer-filter
https://nvd.nist.gov/vuln/de-tail/cve-2026-135738		FFmpeg	Out-of-bounds Write	FFmpeg before 9.1 contains a heap out-of-bounds write vulnerability in libavfilter/vf_signalstats.c that allows attackers to corrupt heap memory by supplying high bit depth samples exceeding the nominal maximum. Attackers can craft planar 9 to 14 bit YUV video whose unclamped samples or saturation values index past histogram ends, crashing applications or possibly executing code.	https://code.ffmpeg.org/FFmpeg/FFmpeg/pulls/26121 https://github.com/FFmpeg/FFmpeg https://github.com/FFmpeg/FFmpeg/blob/n9.0.2/libavfilter/vf_signalstats.c#L620 https://github.com/FFmpeg/FFmpeg/com-mit/04955e8b148fa3e7ab022cbb9f5e35c49165ae21 https://www.vulncheck.com/adviso-ries/ffmpeg-before-9.1-heap-out-of-bounds-write-via-signalstats-filter-histograms
https://nvd.nist.gov/vuln/de-tail/cve-2026-135740		FFmpeg	Out-of-bounds Write	FFmpeg before 9.1 contains a heap out-of-bounds write vulnerability in libavfilter/vf_readeia608.c because build_histogram() does not clamp high bit depth luma samples to the nominal maximum. Attackers can supply crafted 9, 10, 12 or 14 bit gray or YUV video to corrupt heap memory, causing crashes or possibly code execution.	https://code.ffmpeg.org/FFmpeg/FFmpeg/pulls/26121 https://github.com/FFmpeg/FFmpeg https://github.com/FFmpeg/FFmpeg/blob/n9.0.2/libavfilter/vf_readeia608.c#L176 https://github.com/FFmpeg/FFmpeg/com-mit/df1ddf75db9a1ff36a35019511e17f795cf20c55

					https://www.vulncheck.com/advisories/ffmpeg-before-9.1-heap-out-of-bounds-write-via-readeia608-filter-histogram
https://nvd.nist.gov/vuln/detail/cve-2026-135295	7,8	FontForge	Out-of-bounds Write	FontForge through 20251009 contains a heap out-of-bounds write vulnerability in PcfReadEncodingsNames() that allows attackers to corrupt memory via negative glyph indices from truncated PCF encodings tables. Attackers can supply a crafted .pcf file imported through the GUI or scripting Import() command to write before the encs array, causing crashes or potential code execution.	https://github.com/fontforge/fontforge/blob/20251009/fontforge/fvimportbdf.c#L1719-L1755 https://github.com/fontforge/fontforge/commit/65e80b5dfb6691a1c8a532cfbb8ec905949e0c9a https://github.com/fontforge/fontforge/pull/5957 https://www.vulncheck.com/advisories/fontforge-through-20251009-heap-out-of-bounds-write-via-pcf-encodings-table
https://nvd.nist.gov/vuln/detail/cve-2026-130164	7,8	NousResearch	External Control of System or Configuration Setting; Untrusted Search Path	Hermes Agent is an open-source autonomous AI agent built by Nous Research for running tool-using workflows across CLI, desktop, and messaging interfaces. From 0.21.6 to 0.23.1, when Bot Desktop is hosted inside a non-local terminal backend, the agent process reads a backend-writable screen environment file without validating keys or values and merges its entries into the environment of processes started on the agent machine. Specifically, when terminal.backend is set to docker or ssh (or a plugin backend declaring supports_streams) with placement auto or terminal, _published() in tools/bot_desktop/sandbox_host.py accepts arbitrary KEY=VALUE lines from the hermes-bot-desktop env file and propagates them via tools/bot_desktop/runtime.py into the browser harness, computer-use helpers, and local terminal children. Code running inside the terminal backend can therefore set variables such as LD_PRELOAD, DYLD_INSERT_LIBRARIES, or PATH and gain code execution on the agent machine as the gateway user upon a subsequent browser or computer-use spawn, exposing credentials, tokens, and session history under the Hermes home directory. The default local backend, backends that cannot host a screen (Modal, Daytona, and Vercel), and Hermes Cloud in its default configuration are not affected. This issue is fixed in version 0.23.2.	https://github.com/NousResearch/hermes-agent/commit/9c44c34ac74bec800ca25c32e7d5e9b1dd47168d https://github.com/NousResearch/hermes-agent/pull/154487 https://github.com/NousResearch/hermes-agent/security/advisories/GHSA-p22p-9ph6-gmrh
https://nvd.nist.gov/vuln/detail/cve-2026-96457	7,7	Keycloak, Red Hat	Missing Authorization	A flaw was found in the administrative interface of Keycloak, an identity and access management solution. The issue occurs when Fine-Grained Admin Permissions are used to restrict a group administrator from managing specific sub-groups. Due to an incomplete fix for a previous vulnerability, a restricted administrator can bypass these restrictions by moving a forbidden sub-group to the top level of the hierarchy. This allows the attacker to gain unauthorized control over the groups members, potentially leading to a full takeover of the security realm.	https://access.redhat.com/security/cve/CVE-2026-96457 https://bugzilla.redhat.com/show_bug.cgi?id=2539300
https://nvd.nist.gov/vuln/detail/cve-2026-103791	7,6	Dell	Improper Validation of Specified Quantity in Input	Dell Enterprise Sonic Distribution, versions prior to 4.6.1, contains an Improper Input Validation vulnerability. An unauthenticated attacker with adjacent network access could potentially exploit this vulnerability, leading to a denial of service condition.	https://www.dell.com/support/kbdoc/en-us/000535884/dsa-2026-451-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities
https://nvd.nist.gov/vuln/detail/cve-	7,5	Apple	Out-of-bounds Read	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 27.2 and iPadOS 27.2, macOS Golden Gate 27.2, tvOS 27.2, visionOS 27.2. An app may be able to cause unexpected system termination or read kernel memory.	https://support.apple.com/en-us/149230 https://support.apple.com/en-us/149521 https://support.apple.com/en-us/149524 https://support.apple.com/en-us/149526

2026-112465					
https://nvd.nist.gov/vuln/detail/cve-2026-134679	7,5	Cirx08	Missing Authorization	WeddingShare through 1.8.2 contains a missing authorization vulnerability in the anonymous MediaViewerController.GalleryItem action that allows unauthenticated attackers to retrieve item upload paths without the gallery secret key. Attackers can enumerate sequential integer item ids to learn paths and uploader names, then download photos and videos from key-protected galleries served as static files.	https://github.com/Cirx08/WeddingShare/blob/1.8.2/WeddingShare/Controllers/MediaViewerController.cs#L18-L100 https://github.com/Cirx08/WeddingShare/issues/199 https://www.vulncheck.com/advisories/weddingshare-through-1.8.2-missing-authorization-via-mediaviewer-galleryitem
https://nvd.nist.gov/vuln/detail/cve-2026-132147	7,5	Debian	Improper Limitation of a Pathname to a Restricted Directory	An arbitrary file read vulnerability was discovered in debbugs, a bug tracking system based on the active Debian BTS. versions.cgi failed to correctly sanitize package name inputs in found and fixed query parameters. Crafted query parameters could cause version.cgi to output any lines of the target file which contained spaces.	https://salsa.debian.org/debbugs-team/debbugs/-/commit/2fbf06866c9322090675a37aa55e4e7fa560bce0
https://nvd.nist.gov/vuln/detail/cve-2026-101219	7,5	Dell	Heap-based Buffer Overflow	Dell Enterprise Sonic Distribution, versions prior to 4.6.1, contains a heap based buffer overflow. An unauthenticated remote attacker with adjacent network access could potentially exploit this vulnerability, leading to a denial of service condition.	https://www.dell.com/support/kbdoc/en-us/000535884/dsa-2026-451-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities
https://nvd.nist.gov/vuln/detail/cve-2026-103786	7,5	Dell	NULL Pointer Dereference	Dell Enterprise Sonic Distribution, versions prior to 4.6.1, contains a null pointer dereference vulnerability. An unauthenticated remote attacker with adjacent network access could potentially exploit this vulnerability, leading to a denial of service condition.	https://www.dell.com/support/kbdoc/en-us/000535884/dsa-2026-451-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities
https://nvd.nist.gov/vuln/detail/cve-2026-103789	7,5	Dell	Heap-based Buffer Overflow	Dell Enterprise Sonic Distribution, versions prior to 4.6.1, contains a heap based buffer overflow. An unauthenticated remote attacker with adjacent network access could potentially exploit this vulnerability, leading to a denial of service condition.	https://www.dell.com/support/kbdoc/en-us/000535884/dsa-2026-451-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities
https://nvd.nist.gov/vuln/detail/cve-2026-82303	7,5	Elastic	Buffer Over-read	A buffer over-read vulnerability in Elasticsearch transport decompression can expose data from other requests. The LZ4 decoder can read beyond the declared compressed block into a shared network buffer. A remote attacker who can reach an affected transport interface can send a specially crafted compressed request and obtain data from outside their own request. Exploitation of the exposed remote-cluster transport interface does not require authentication.	https://discuss.elastic.co/t/391840
https://nvd.nist.gov/vuln/detail/cve-	7,5	FFmpeg	Numeric Truncation Error	FFmpeg before 9.1 contains a heap buffer overflow vulnerability in recv_msg() of the zmq and azmq filters that allows unauthenticated network attackers to corrupt memory by sending oversized command messages. Attackers can send a 4 GiB message to the default listening port, truncating the int buffer size so memcpy() writes past the heap allocation and crashes FFmpeg.	https://code.ffmpeg.org/FFmpeg/FFmpeg/pulls/26081 https://github.com/FFmpeg/FFmpeg https://github.com/FFmpeg/FFmpeg/blob/n9.0.2/libavfilter/f_zmq.c#L138

2026-135742					https://github.com/FFmpeg/FFmpeg/commit/78afb1d6e99ba2d3264f053ae4c0e4487a9c824c https://www.vulncheck.com/advisories/ffmpeg-before-9.1-integer-truncation-via-zmq-filter-recv-msg
https://nvd.nist.gov/vuln/detail/cve-2026-134456	7,5	HyNetworks	Allocation of Resources Without Limits or Throttling	Hysteria 2.5.0 before 2.9.2 contains a denial of service vulnerability in the HTTP sniff implementation that fails to limit header size. Attackers can continuously send excessively large HTTP headers without terminating them, exhausting server memory and causing out-of-memory crashes.	https://github.com/HyNetworks/hysteria/security/advisories/GHSA-jqc5-2p7q-fqfc https://www.vulncheck.com/advisories/hysteria-2.5.0-before-2.9.2-denial-of-service-via-http-sniff-header
https://nvd.nist.gov/vuln/detail/cve-2026-120787	7,5	Microsoft	Improper Certificate Validation	Improper certificate validation in Microsoft Office PowerPoint allows an unauthorized attacker to execute code over a network.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-120787
https://nvd.nist.gov/vuln/detail/cve-2026-134843	7,5	pgjdbc	Improper Neutralization of Special Elements used in an SQL Command; Improper Handling of Exceptional Conditions	pgjdbc, the PostgreSQL JDBC Driver, does not close the connection when an unchecked exception interrupts a request. Part of a Bind message stays in the send buffer, and the server reads the bytes that follow as the rest of it. The bytes of a value uploaded later on the same connection can then run as a SQL command. Since 42.6.0 a setBinaryStream() value without a length that is executed again throws such an exception, as does the driver's own retry after SQLState 0A000 or 26000. An application stream that throws an unchecked exception has the same effect in all versions. All versions before 42.7.15 are affected, and 42.7.15 fixes the problem.	https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-cww3-qmc2-mjmr
https://nvd.nist.gov/vuln/detail/cve-2026-134844	7,5	pgjdbc	Uncontrolled Search Path Element	pgjdbc, the PostgreSQL JDBC Driver, uses unqualified operators and functions in the catalog queries of DatabaseMetaData, ResultSetMetaData and TypeInfoCache. A role with CREATE on a schema of the application's search_path can add an operator with an exact type match, and the server runs it with the privileges of the application's role. TypeInfoCache also resolves an unqualified type name such as interval by its own ranking. A domain with that name in another schema, even the temporary schema of another session, can be used instead, and its CHECK runs in the application's session. All versions before 42.7.15 are affected, and 42.7.15 fixes the problem.	https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-j75g-99q3-vr5c
https://nvd.nist.gov/vuln/detail/cve-2026-134364	7,5	py-pdf	Exposure of Sensitive Information to an Unauthorized Actor	pypdf 3.7.1 before 7.0.0 contains an information disclosure vulnerability that allows attackers to guess placeholders in encrypted templated documents by analyzing file identifiers. Attackers with a document sharing the same template and access to other documents' file identifiers can recover placeholder contents from encrypted PDFs.	https://github.com/py-pdf/pypdf/security/advisories/GHSA-mwj3-fpmc-hjcv https://www.vulncheck.com/advisories/pypdf-3.7.1-before-7.0.0-placeholder-recovery-via-file-identifier-in-encrypted-documents
https://nvd.nist.gov/vuln/detail/cve-2026-134366	7,5	py-pdf	Inefficient Algorithmic Complexity	pypdf before 7.0.0 contains a resource exhaustion vulnerability that allows attackers to cause large memory usage by supplying crafted PDF cross-reference streams. Attackers can craft a PDF whose cross-reference stream offsets all point to one large object, exhausting memory in applications parsing the file.	https://github.com/py-pdf/pypdf/security/advisories/GHSA-59jv-x5x2-gg4c https://www.vulncheck.com/advisories/pypdf-before-7.0.0-memory-exhaustion-via-cross-reference-streams-with-identical-offsets

https://nvd.nist.gov/vuln/detail/cve-2026-134367	7,5	py-pdf	Allocation of Resources Without Limits or Throttling	pypdf 2.4.2 before 7.0.0 contains a resource exhaustion vulnerability in its handling of XFA forms that allows attackers to cause excessive memory consumption. Attackers can supply a crafted PDF containing XFA forms with many small fields so that loading the forms consumes large amounts of memory, causing a denial of service.	https://github.com/py-pdf/pypdf/security/advisories/GHSA-cmpx-464x-82c3 https://www.vulncheck.com/advisories/pypdf-2.4.2-before-7.0.0-excessive-memory-usage-via-xfa-forms
https://nvd.nist.gov/vuln/detail/cve-2026-129837	7,5	Red Hat	Out-of-bounds Read	A flaw was found in rsyslog. A remote, unauthenticated attacker can cause a Denial of Service (DoS) by sending a specially crafted log message with an unusual timestamp. When the service processes this message using weekday formatting templates, an out-of-bounds memory read occurs, causing the application to crash.	https://access.redhat.com/security/cve/CVE-2026-129837 https://bugzilla.redhat.com/show_bug.cgi?id=2579411 http://www.openwall.com/lists/oss-security/2026/11/17/13 http://www.openwall.com/lists/oss-security/2026/11/17/8
https://nvd.nist.gov/vuln/detail/cve-2026-59442	7,5	Spring	Not specified	TypesenseFilterExpressionConverter does not correctly translate grouped (parenthesized) filter expressions into the Typesense filter syntax. As a result, the filter sent to Typesense can have a different meaning than the one the application defined, and some conditions may not be applied as intended. An application is affected if it uses the Typesense vector store with filter expressions that contain groups and relies on them to restrict results, for example to enforce tenant isolation or access control. In that case, a remote user may be able to retrieve documents they should not have access to, and the same filter used for a delete operation may remove documents outside the intended scope.	https://spring.io/security/cve-2026-59442
https://nvd.nist.gov/vuln/detail/cve-2026-119114	7,4	emrevona	Improper Limitation of a Pathname to a Restricted Directory	The WP Fastest Cache – WordPress Cache Plugin plugin for WordPress is vulnerable to arbitrary directory deletion due to insufficient file path validation in the singleDeleteCache function in all versions up to, and including, 1.5.4 This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). Successful exploitation requires either the Custom Permalinks plugin or the GeoDirectory plugin to be co-installed, as these provide the necessary mechanism to write a traversal-bearing permalink value into the database that WP Fastest Cache then consumes without validation.	https://plugins.trac.wordpress.org/browser/wp-fastest-cache/tags/1.5.3/wpFastestCache.php#L1389 https://plugins.trac.wordpress.org/browser/wp-fastest-cache/tags/1.5.3/wpFastestCache.php#L1501 https://plugins.trac.wordpress.org/browser/wp-fastest-cache/tags/1.5.3/wpFastestCache.php#L1517 https://plugins.trac.wordpress.org/browser/wp-fastest-cache/tags/1.5.3/wpFastestCache.php#L1627 https://plugins.trac.wordpress.org/browser/wp-fastest-cache/tags/1.5.3/wpFastestCache.php#L1718 https://plugins.trac.wordpress.org/browser/wp-fastest-cache/tags/1.5.3/wpFastestCache.php#L2406 https://plugins.trac.wordpress.org/changeset/3780060/wp-fastest-cache/trunk/wpFastestCache.php https://plugins.trac.wordpress.org/changeset/3786304/wp-fastest-

					cache/trunk/wpFastestCache.php https://www.wordfence.com/threat-intel/vulnerabilities/id/2925032b-2a0c-43b6-a719-27831be34d19?source=cve
https://nvd.nist.gov/vuln/detail/cve-2026-134454	7,4	HyNetworks	Improper Access Control	Hysteria from 2.0.0 before 2.9.2 contains an ACL bypass vulnerability that allows authenticated clients to reach blocked UDP destinations by reusing an established UDP session. Attackers can open a session to an allowed destination, then send later packets to localhost or private-network addresses to access internal-only UDP services.	https://github.com/HyNetworks/hysteria/security/advisories/GHSA-vgrc-hq28-p3xp https://www.vulncheck.com/advisories/hysteria-2.0.0-before-2.9.2-udp-acl-bypass-enabling-ssrf
https://nvd.nist.gov/vuln/detail/cve-2026-134845	7,4	pgjdbc	Improper Certificate Validation; Cleartext Transmission of Sensitive Information	pgjdbc, the PostgreSQL JDBC Driver, does not enforce TLS for some settings that ask for it. When sslmode is not set, an ssl value such as 1, on, yes or verify-full gives sslmode=prefer, or no TLS before 42.2.5. A service given in the Properties instead of the URL is ignored, so the sslmode of its pg_service.conf entry is lost. BaseDataSource.setUrl() keeps an sslmode, channelBinding or gssEncMode that was set before it. An attacker on the network path can then read and change the traffic. Versions 9.4.1208 through 42.7.14 are affected, and 42.7.15 fixes the problem.	https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-3mrw-838h-x9j9
https://nvd.nist.gov/vuln/detail/cve-2026-134848	7,4	pgjdbc	Improper Neutralization of Null Byte or NUL Character	pgjdbc, the PostgreSQL JDBC Driver, does not refuse a NUL character in a startup parameter. The StartupMessage is a list of NUL-terminated strings, so a NUL in the database name, user, currentSchema, options or ApplicationName adds further parameters. %00 in a URL decodes to a NUL. Someone who controls part of the URL or a property can choose another login role or add replication=database, although the connection still has to pass the authentication of that role. On a server that trusts the client, the attacker can log in as any role. All versions before 42.7.15 are affected, and 42.7.15 fixes the problem.	https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-36wf-f6m2-v42m
https://nvd.nist.gov/vuln/detail/cve-2026-135686	7,4	Trilium Next	Improper Neutralization of Special Elements used in an SQL Command	Trilium through 0.107.0 contains an sql injection vulnerability in updateNormalEntity() that allows malicious sync partners to inject SQL by supplying crafted entity names and column keys. Attackers can abuse /api/sync/changed or PUT /api/sync/update data to copy sessions, etapi_tokens and user_data into synced rows and write arbitrary database rows.	https://github.com/TriliumNext/Trilium https://github.com/TriliumNext/Trilium/blob/v0.107.0/packages/trilium-core/src/services/sync_update.ts#L107 https://github.com/TriliumNext/Trilium/commit/4ec30088fce936f2e87c0af6af3f89c47d331176 https://www.vulncheck.com/advisories/trilium-through-0.107.0-sql-injection-via-sync-update-entity-name
https://nvd.nist.gov/vuln/detail/cve-2026-134069	7,3	AWS	Use of Default Cryptographic Key	Use of a default cryptographic key in the instance registration component in Amazon SSM Agent before 3.3.5226.0 on AWS-provided Windows Server AMIs released before 2026-09-09 might allow local users without administrative privileges to obtain the instance's Default Host Management Configuration role credentials via the registration key shared by all instances launched from the same AMI. To remediate this issue, users should replace affected instances with instances launched from AWS Windows Server AMIs released on or after 2026-09-09, which include SSM Agent 3.3.5226.0 or later. Upgrading the agent in place does not replace the shared key, and deleting the agent's Vault breaks instances managed through Default Host Management Configuration.	https://aws.amazon.com/security/security-bulletins/2026-197-aws/ https://github.com/aws/amazon-ssm-agent/releases/tag/3.3.5226.0 https://github.com/aws/amazon-ssm-agent/security/advisories/GHSA-rfpp-9v45-jjv4
https://nvd.nist.gov/vuln/detail/cve-	7,2	itpathsolutions	Improper Neutralization of Input During Web Page Generation	The Contact Form to Any API plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'your-message (any CF7 form field)' parameter in all versions up to, and including, 3.0.7 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	https://plugins.trac.wordpress.org/browser/contact-form-to-any-api/tags/3.0.7/admin/class-cf7-to-any-api-admin.php#L640

2026-131822				malicious payload is stored via a single unauthenticated POST to Contact Form 7's public REST feedback endpoint, which uses permission_callback __return_true and requires no authentication or prior interaction to submit.	https://plugins.trac.wordpress.org/browser/contact-form-to-any-api/tags/3.0.7/admin/class-cf7-to-any-api-admin.php#L759 https://plugins.trac.wordpress.org/browser/contact-form-to-any-api/tags/3.0.7/admin/partials/cf7-to-any-api-admin-entries.php#L115 https://plugins.trac.wordpress.org/browser/contact-form-to-any-api/tags/3.0.7/includes/class-cf7-to-any-api.php#L181 https://plugins.trac.wordpress.org/changeset?reponame=&old=3811674%40contact-form-to-any-api&new=3811674%40contact-form-to-any-api https://www.wordfence.com/threat-intel/vulnerabilities/id/3c0753da-2807-46d1-b002-d557e7f3bf13?source=cve
https://nvd.nist.gov/vuln/detail/cve-2026-124216	7,2	iworks	Improper Neutralization of Input During Web Page Generation	The Orphans plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'comment' parameter in all versions up to, and including, 3.4.5 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. Exploitation requires a two-step comment chain: a benign first comment must be approved under a given name and email so that WordPress's comment_previously_approved mechanism auto-publishes the attacker's payload comment without moderation.	https://github.com/iworks/sierotki/releases/tag/3.4.6 https://plugins.trac.wordpress.org/browser/sierotki/tags/3.4.5/includes/iworks/class-iworks-orphan.php#L266 https://plugins.trac.wordpress.org/browser/sierotki/tags/3.4.5/includes/iworks/class-iworks-orphan.php#L484 https://plugins.trac.wordpress.org/browser/sierotki/tags/3.4.5/includes/iworks/class-iworks-orphan.php#L502 https://plugins.trac.wordpress.org/browser/sierotki/tags/3.4.5/includes/iworks/class-iworks-orphan.php#L572 https://plugins.trac.wordpress.org/browser/sierotki/tags/3.4.5/wp-comments-post.php%20%28core%29 https://www.wordfence.com/threat-intel/vulnerabilities/id/d313cb15-59f4-4483-ba4b-d2237fa33248?source=cve
https://nvd.nist.gov/vuln/detail/cve-2026-134817	7,1	Flux159	Improper Neutralization of Argument Delimiters in a Command	mcp-server-kubernetes before 4.2.0 contains an argument injection vulnerability that allows remote MCP clients to inject kubectl flags by supplying dash-prefixed values as positional operands in tools such as exec_in_pod, kubectl_patch, and kubectl_logs. Attackers connected over SSE or Streamable HTTP transport can supply values like --filename to make kubectl read files from the server host, bypassing file-read restrictions.	https://github.com/Flux159/mcp-server-kubernetes/blob/v4.1.9/src/tools/exec_in_pod.ts#L105 https://github.com/Flux159/mcp-server-kubernetes/commit/588d4949b0233974c3966a7d24d532be11

					e56d0d https://github.com/Flux159/mcp-server-kubernetes/pull/390 https://github.com/Flux159/mcp-server-kubernetes/releases/tag/v4.2.0 https://www.vulncheck.com/advisories/mcp-server-kubernetes-before-4.2.0-argument-injection-via-flag-shaped-positional-operands
https://nvd.nist.gov/vuln/detail/cve-2026-131793	7,1	IT Path Solutions	Improper Neutralization of Input During Web Page Generation	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in IT Path Solutions Contact Form to Any API contact-form-to-any-api allows Stored XSS.This issue affects Contact Form to Any API: from n/a through 3.0.7.	https://patchstack.com/database/wordpress/plugin/contact-form-to-any-api/vulnerability/wordpress-contact-form-to-any-api-plugin-3-0-7-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/cve-2026-120777	7,1	Microsoft	Incorrect Authorization	Incorrect authorization in Azure Managed Service Identity allows an authorized attacker to elevate privileges over a network.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-120777
https://nvd.nist.gov/vuln/detail/cve-2026-131742	7,1	PluginUs.Net	Improper Neutralization of Input During Web Page Generation	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PluginUs.Net Active Products Tables for WooCommerce profit-products-tables-for-woocommerce allows Reflected XSS.This issue affects Active Products Tables for WooCommerce: from n/a through 2.1.8.	https://patchstack.com/database/wordpress/plugin/profit-products-tables-for-woocommerce/vulnerability/wordpress-active-products-tables-for-woocommerce-plugin-2-1-8-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/cve-2026-131772	7,1	PluginUs.Net	Improper Neutralization of Input During Web Page Generation	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PluginUs.Net HUSKY woocommerce-products-filter allows Stored XSS.This issue affects HUSKY: from n/a through 1.4.8.	https://patchstack.com/database/wordpress/plugin/woocommerce-products-filter/vulnerability/wordpress-husky-plugin-1-4-8-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/cve-2026-129801	7,1	RT-Labs AB	Out-of-bounds Read	The FoE DATA frame handler computes the payload length from the master-supplied mailbox length field and passes it directly to FOE_fwrite. The length is checked against the remaining file capacity but not against the physical mailbox buffer size. A master can declare a large length while sending a short frame, causing FOE_fwrite to read past the end of the mailbox buffer.	https://docs.rt-labs.com/security/advisories/rrtl-261119-01.html
https://nvd.nist.gov/vuln/detail/cve-2026-135706	7,0	FFmpeg	Heap-based Buffer Overflow	FFmpeg before 9.1 contains a heap buffer overflow vulnerability in modplug_read_header() in libavformat/libmodplug.c that allocates the buffer using max_size instead of sz. When max_size is set to 0, attackers can supply crafted module files that avio_read() copies into a zero-sized buffer, causing memory corruption, crashes, or possible code execution.	https://code.ffmpeg.org/FFmpeg/FFmpeg/pulls/24914 https://github.com/FFmpeg/FFmpeg https://github.com/FFmpeg/FFmpeg/blob/n9.0.2/libavformat/libmodplug.c#L200 https://github.com/FFmpeg/FFmpeg/commit/edc96a209b25b78d3e4b96e951774eb13c

					8da0b0 https://www.vulncheck.com/advisories/ffmpeg-before-9.1-heap-buffer-overflow-via-libmodplug-demuxer
https://nvd.nist.gov/vuln/detail/cve-2026-135709	7,0	FFmpeg	Out-of-bounds Write	FFmpeg before 9.1 contains an out-of-bounds write vulnerability in ogg_buffer_data() in libavformat/oggenc.c because ogg_buffer_page() leaves a full page current after failed allocation. When page allocation fails, a memset with length (size_t)-1 or an overflowing memcpy writes past the segment table, causing heap memory corruption and crashes when writing Ogg output.	https://code.ffmpeg.org/FFmpeg/FFmpeg/pulls/24932 https://github.com/FFmpeg/FFmpeg https://github.com/FFmpeg/FFmpeg/blob/n9.0.2/libavformat/oggenc.c#L252 https://github.com/FFmpeg/FFmpeg/commit/6d40aa17395aaba80922441bcfb58399a88475e3 https://github.com/FFmpeg/FFmpeg/commit/a659cd842b122e2f41973ac7c4e826426cc0d756 https://www.vulncheck.com/advisories/ffmpeg-before-9.1-out-of-bounds-write-via-ogg-buffer-data-in-oggenc-c
https://nvd.nist.gov/vuln/detail/cve-2026-135723	7,0	FFmpeg	Double Free	FFmpeg before 9.1 contains a double free vulnerability in the fill_marker() function of libavformat/imf_cpl.c that frees a Marker label without clearing the pointer when default scope allocation fails. Attackers can supply a crafted Composition Playlist with a Marker Label lacking a scope attribute, triggering a second free in imf_marker_free() under memory pressure and causing memory corruption or a crash.	https://code.ffmpeg.org/FFmpeg/FFmpeg/pulls/24917 https://github.com/FFmpeg/FFmpeg https://github.com/FFmpeg/FFmpeg/blob/n9.0.2/libavformat/imf_cpl.c#L315 https://github.com/FFmpeg/FFmpeg/commit/301a611370a0ba81f4a71d3b7ccd064623606c1b https://www.vulncheck.com/advisories/ffmpeg-before-9.1-double-free-in-imf-cpl-parser-fill-marker

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 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
CISA Adds Four Known Exploited Vulnerabilities to Catalog	▪ CVE-2025-42884 SAP NetWeaver Improper Neutralization of Special Elements in Data Query Logic Vulnerability ▪ CVE-2026-76466 Cisco Expressway Series Use of Hard-coded Credentials Vulnerability ▪ CVE-2026-123890 VMWare vCenter Authentication Bypass Using an Alternate Path or Channel Vulnerability ▪ CVE-2026-129448 Apache Roller Deserialization of Untrusted Data Vulnerability	https://www.cisa.gov/news-events/alerts/2026/11/20/cisa-adds-four-known-exploited-vulnerabilities-catalog
CISA Adds Two Known Exploited Vulnerabilities to Catalog	▪ CVE-2026-133968 Project MONAI MONAI Label Path Traversal Vulnerability ▪ CVE-2026-134624 N-able Mail Assure (SpamExperts) Server-Side Request Forgery (SSRF) Vulnerability	https://www.cisa.gov/news-events/alerts/2026/11/23/cisa-adds-two-known-exploited-vulnerabilities-catalog
Vulnerability Summary for the Week of September 21, 2026		https://www.cisa.gov/news-events/bulletins/sb26-271

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
Signal Restricts Screenshots to protect User Privacy from AI assistants	https://cybersecuritynews.com/signal-restricts-screen-shots/
Meta AI Agent Muse Reads Encrypted Messages Through Android Notifications and Mac Permissions	https://cybersecuritynews.com/muse-reads-encrypted-messages/
CrowdStrike in Talks to Acquire Zscaler in One of the Biggest Cybersecurity Deals Ever	https://cybersecuritynews.com/crowdstrike-to-acquire-zscaler/
Microsoft Investigates Attachment Upload Failures in New Outlook	https://cybersecuritynews.com/microsoft-attachment-upload-failures/
Russian National Accused of Using Remote Access Tools to Spy on Silicon Valley Defense Firm	https://cybersecuritynews.com/russian-national-silicon-valley-spy/
Jensen Huang Returns as NVIDIA CEO Following Unanimous Board Vote	https://cybersecuritynews.com/nvidia-reinstates-jensen-huang/
CrowdStrike to Acquire Zscaler in Massive $43.9 Billion Cybersecurity Deal	https://cybersecuritynews.com/crowdstrike-acquire-zscaler/

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
Samsung Securities Data Breach Exposes 8,241 Customers' Personal and Account Details	https://cybersecuritynews.com/samsung-securities-data-breach/
Hackers Use Autonomous AI to Breach 10 Organizations and Access Over 1 Million Personal Records	https://cybersecuritynews.com/hackers-use-autonomous-ai/
JPMorgan Chase Confirms Third-Party Cyberattack That May Have Exposed Customer Names and Emails	https://cybersecuritynews.com/jpmorgan-third-party-data-breach/
Cleverbridge Confirms Hackers Stole Customer Card Numbers and CVV Codes in a Major Data Breach	https://cybersecuritynews.com/cleverbridge-data-breach/
KPMG Canada Confirms Cyberattack as Hackers Access Confidential Client Tax Documents	https://cybersecuritynews.com/kpmg-canada-confirms-cyberattack/
European Commission Disables Access to EU Academy After Cyberattack Exposes User Data	https://cybersecuritynews.com/eu-academy-disabled/
Hackers Leak Customer Data Linked to Visa, Mastercard and JPMorgan After Third-Party Cyberattacks	https://cybersecuritynews.com/visa-mastercard-jpmorgan-data-breach/
Hackers Breach TfL Oyster Photocard Accounts, Exposing Personal Data of 265,000 Customers	https://cybersecuritynews.com/hackers-breach-tfl-oyster-photocard-accounts/
OpenRouter Users' Private AI Chats Possibly Exposed Via Compromised Third-Party Providers	https://cybersecuritynews.com/openrouter-ai-chat-leaks/
Hackers Secretly Spy on Bulgarian Government for Five Years and Steal 62 Million Pages of Documents	https://cybersecuritynews.com/bulgarian-government/
Jailbroken AI Agent Helps Hacker Steal Customer Data and 8.6GB of European Government Files	https://cybersecuritynews.com/jailbroken-ai-agent/

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
Critical Apache Tomcat Flaw Lets Remote Attackers Join Trusted Server Clusters Without Authentication	https://cybersecuritynews.com/critical-apache-tomcat-flaw/
Hackers Allegedly Claiming Exploit for VMware vCenter 0-day Vulnerability	https://cybersecuritynews.com/alleged-vmware-vcenter-0-day-exploit/
Researchers Hack Volkswagen Cars via Bluetooth to Spy on Conversations and Track GPS Locations	https://cybersecuritynews.com/hack-volkswagen-cars-via-bluetooth/
Critical Node.js simple-git Library Vulnerability Enables Remote Code Execution Attacks	https://cybersecuritynews.com/node-js-simple-git-library-flaw/
PHP Warns of Critical Security Flaws Affecting All Supported Versions, Urges Users to Update	https://cybersecuritynews.com/php-8-released/
Hackers Actively Exploiting Cisco Expressway Vulnerability to Gain Full Root Access	https://cybersecuritynews.com/cisco-expressway-vulnerability-exploited/
Critical VMware vCenter Flaws Let Hackers Bypass Authentication and Access Servers	https://cybersecuritynews.com/vmware-vcenter-authentication-bypass/
New phpAfterShell Attack Bypasses PHP2Shell Fix to Enable Remote Code Execution	https://cybersecuritynews.com/phpaftershell-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/
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/
8.8 Million NGINX Services Still Potentially Exposed to Critical NGINX2Root Vulnerability	https://cybersecuritynews.com/nginx2root-vulnerability/
OpenAI’s GPT-6.2 Astra Discovers 0-Day Vulnerabilities Enabling Mobile OS Security Bypass and RCE	https://cybersecuritynews.com/openai-gpt-6-2-astra-0-day-vulnerabilities/

Σύντομη περιγραφή / Τίτλος	URL
Hackers Exploit GL.iNet Cloud Flaw to Install Malware on Routers and KVM Devices	https://cybersecuritynews.com/hackers-exploit-gl-inet-cloud-flaw/
Hackers Exploit Critical Cisco Expressway Flaw to Gain Root Access and Infiltrate Internal Networks	https://cybersecuritynews.com/hackers-exploit-critical-cisco-expressway-flaw/
Hackers Could Execute Commands on WordPress, Email and Print Servers Through Upload2Shell Flaw	https://cybersecuritynews.com/upload2shell-flaw/
Hackers Actively Scan LiteLLM AI Servers for Critical Flaws Enabling RCE Attacks	https://cybersecuritynews.com/litellm-ai-servers/
Hackers Exploit Microsoft Entra Connect Health Flaw to Access Admin Emails and Organization Data	https://cybersecuritynews.com/microsoft-entra-connect-health-flaw/
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/
WhatsApp Android Flaws Could Let Hackers Delete Users' Files and Expose IP Addresses	https://cybersecuritynews.com/whatsapp-android-flaws/
Palo Alto Confirms Java Vulnerability Impacts Privilege Threat Analytics and Remote Access Connector	https://cybersecuritynews.com/palo-alto-confirms-java-vulnerability-impacts/
Critical ASP.NET AntiCsrf Flaw Under Attack, Allowing Hackers to Execute Code Without Login	https://cybersecuritynews.com/asp-net-anticsrf-flaw-under-attack/
iTerm2 Remote Code Execution Flaw Lets Hackers Run Malicious Commands by Displaying Crafted Files	https://cybersecuritynews.com/iterm2-remote-code-execution-flaw/
Over 100 Debian Packages Still Contain Distrusted CA Certificates Despite Security Updates	https://cybersecuritynews.com/debian-packages-ca-certificates/
OpenSSL Hit by Critical 9.8 Heap Buffer Overflow Vulnerability in Base64 Encoding Function	https://cybersecuritynews.com/openssl-heap-buffer-overflow/
Hackers Use AI to Discover Zero-Day in 11 Minutes, Then Take Full Control of Server	https://cybersecuritynews.com/hackers-use-ai/
6 Critical F5 BIG-IP Vulnerabilities Could Let Hackers Disrupt Websites and Execute Malicious Code	https://cybersecuritynews.com/critical-f5-big-ip-vulnerabilities/

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
Palo Alto Confirms NGINX Vulnerabilities Impact PAN-OS and Releases Workarounds	https://cybersecuritynews.com/palo-alto-confirms-nginx-rce-vulnerabilities/
Drupal Fixes Critical RCE Flaw That Could Let Unauthenticated Hackers Take Over Websites	https://cybersecuritynews.com/drupal-fixes-critical-rce-flaw/
Wireshark 4.6.10 Released With Patch for 39 Security Vulnerabilities	https://cybersecuritynews.com/wireshark-4-6-10-released/
ClamAV Patches 10 High-Severity Vulnerabilities That Could Let Attackers Crash Antivirus Scanners	https://cybersecuritynews.com/clamav-patches-10-high-severity-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 480+ Malicious Ad Domains to Target iPhones and Steal Crypto Wallet Recovery Phrases	https://cybersecuritynews.com/malicious-ad-domains-target-iphones/
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 Billion Fraudulent Ad Requests Daily	https://cybersecuritynews.com/badbox-3-0-malware/
Hackers Hide RevStealer Malware in Fake Claude AI App to Steal Passwords and Crypto Wallets	https://cybersecuritynews.com/hackers-hide-revstealer-malware/
Hackers Use AI-Assisted PowerShell Toolkit With 41 Modules to Target African Stock Exchange	https://cybersecuritynews.com/ai-assisted-powershell/
Vmcloudoor Malware Could Let Hackers Secretly Control Linux Cloud Servers and Steal Sensitive Files	https://cybersecuritynews.com/vmcloudoor-malware/

Σύντομη περιγραφή / Τίτλος	URL
Hackers Exploit Misconfigured Temenos Banking Platform to Deploy Web Shells Without Passwords	https://cybersecuritynews.com/temenos-banking-platform/
Hackers Use AI-Powered ARTEX Framework to Automate Cyberattacks Without Relying on Zero-Day Exploits	https://cybersecuritynews.com/hackers-use-ai-powered-artex-framework/
BYOD Ransomware Hackers Play Audio Ransom Messages on Computers Across Hospitals and Universities	https://cybersecuritynews.com/byod-ransomware/
Hackers Turn Legitimate VPN Software Into a Stealthy Tool for Spying on Government Networks	https://cybersecuritynews.com/legitimate-vpn-software/
Hackers Plant 13 ClickFix Traps on Compromised WordPress Site to Trick Visitors Into Running Malware	https://cybersecuritynews.com/hackers-plant-13-clickfix-traps/
Hackers Use 355 Domains to Spread Fake GTA 6 PC Launchers Delivering Malware	https://cybersecuritynews.com/fake-gta-6-pc-launchers/

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
Indian Cyber Crime Coordination Center Urges Users Not to Share Confidential Data on WhatsApp Web	https://cybersecuritynews.com/whatsapp-web-confidential-data/
VirusTotal’s New Ransomware Detection Catches Malware Missed by All 75 Antivirus Engines	https://cybersecuritynews.com/virustotal-ransomware-detection/
OpenAI and Cisco Launch Shirudo AI Security Tool to Block Exploits on Linux Servers	https://cybersecuritynews.com/openai-and-cisco-launch-shirudo/

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/