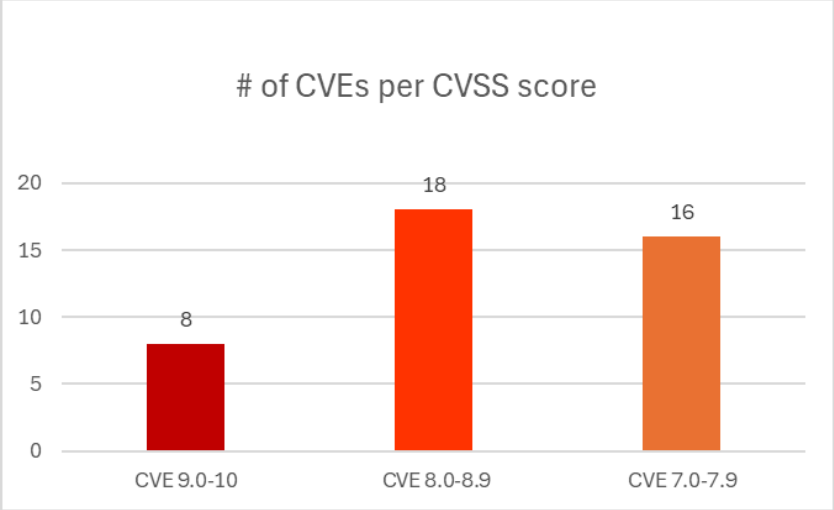
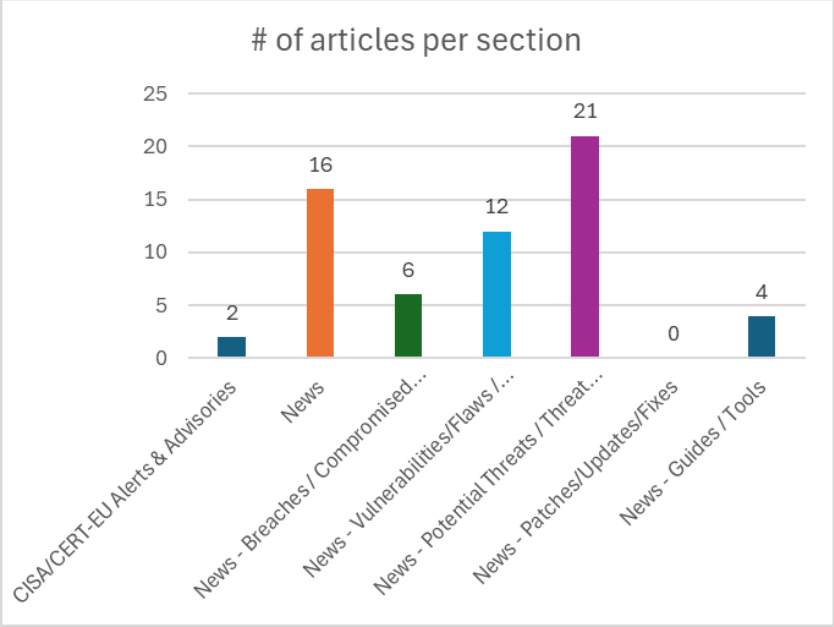
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 01/04/2026 - 03/04/2026





Contents

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 της ευπάθειας (όπως SQL injection ή command injection) και σχετικοί σύνδεσμοι για περαιτέρω πληροφόρηση ή μέτρα αντιμετώπισης.

URL ευπάθειας (NIST NVD)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2026-34717	9,8	OpenProject	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Prior to version 17.2.3	https://github.com/opf/openproject/releases/tag/v17.2.3 https://github.com/opf/openproject/security/advisories/GHSA-5rrm-6qmq-2364
https://nvd.nist.gov/vuln/detail/CVE-2026-34877	9,8	Mbed TLS	Execution with Unnecessary Privileges	Mbed TLS versions from 2.19.0 up to 3.6.5, Mbed TLS 4.0.0	https://mbed-tls.readthedocs.io/en/latest/security-advisories/ https://mbed-tls.readthedocs.io/en/latest/security-advisories/mbedtls-security-advisory-2026-03-serialized-data/
https://nvd.nist.gov/vuln/detail/CVE-2026-5288	9,6	WebView in Google Chrome	Use After Free	WebView in Google Chrome on Android prior to 146.0.7680.178	https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html https://issues.chromium.org/issues/495507390
https://nvd.nist.gov/vuln/detail/CVE-2026-5289	9,6	Navigation in Google Chrome	Use After Free	Navigation in Google Chrome prior to 146.0.7680.178	https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html https://issues.chromium.org/issues/495931147
https://nvd.nist.gov/vuln/detail/CVE-2026-5290	9,6	Compositing in Google Chrome	Use After Free	Compositing in Google Chrome prior to 146.0.7680.178	https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html Chrome https://issues.chromium.org/issues/496205576
https://nvd.nist.gov/vuln/detail/CVE-2026-34532	9,1	Parse Server	Incorrect Authorization	Prior to versions 8.6.67 and 9.7.0-alpha.11	https://github.com/parse-community/parse-server/commit/4fc48cf28f22eea200d74d883505f485234a48d7 https://github.com/parse-community/parse-server/commit/dc59e272665644083c5b7f6862d88ce1ef0b2674 https://github.com/parse-community/parse-server/pull/10342 https://github.com/parse-community/parse-server/pull/10343 https://github.com/parse-community/parse-server/security/advisories/GHSA-vpj2-qq7w-5qq6
https://nvd.nist.gov/vuln/detail/CVE-2026-34872	9,1	Mbed TLS	Improper Verification of Cryptographic Signature	Mbed TLS 3.5.x and 3.6.x through 3.6.5 and TF-PSA-Crypto 1.0	https://mbed-tls.readthedocs.io/en/latest/security-advisories/ https://mbed-tls.readthedocs.io/en/latest/security-advisories/mbedtls-security-advisory-2026-03-ffdh-peerkey-checks/
https://nvd.nist.gov/vuln/detail/CVE-2026-34873	9,1	Mbed TLS	Improper Authentication	Mbed TLS 3.5.0 through 4.0.0	https://mbed-tls.readthedocs.io/en/latest/security-advisories/ https://mbed-tls.readthedocs.io/en/latest/security-advisories/mbedtls-security-advisory-2026-03-client-impersonation-while-resuming-tls13-session/

https://nvd.nist.gov/vuln/detail/CVE-2025-13855	8,8	IBM	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	IBM Storage Protect Server 8.2.0 IBM Storage Protect Plus Server	https://www.ibm.com/support/pages/node/7267783
https://nvd.nist.gov/vuln/detail/CVE-2026-20094	8,8	Cisco	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Cisco IMC	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-3hKN3bVt
https://nvd.nist.gov/vuln/detail/CVE-2026-34797	8,8	Endian Firewall	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Endian Firewall version 3.3.25 and prior	https://help.endian.com/hc/en-us/sections/360004371358-Community https://www.vulncheck.com/advisories/endian-firewall-cgi-bin-logs-smtp-cgi-date-perl-command-injection
https://nvd.nist.gov/vuln/detail/CVE-2026-5204	8,8	Tenda	Out-of-bounds Write	Tenda CH22 1.0.0.1	https://github.com/Litengzheng/vuldb_new/blob/main/CH22/vul_49/README.md https://vuldb.com/submit/780209 https://vuldb.com/vuln/354332 https://vuldb.com/vuln/354332/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-5212	8,8	D-Link	Out-of-bounds Write	D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20260205	https://github.com/wudipjq/my_vuln/blob/main/D-Link8/vuln_166/166.md VulDB Exploit Third Party Advisory https://vuldb.com/submit/780435 https://vuldb.com/submit/780436 https://vuldb.com/vuln/354348 https://vuldb.com/vuln/354348/cti https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-5213	8,8	D-Link	Out-of-bounds Write	D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20260205	https://github.com/wudipjq/my_vuln/blob/main/D-Link8/vuln_168/168.md https://vuldb.com/submit/780437 https://vuldb.com/vuln/354350 https://vuldb.com/vuln/354350/cti https://www.dlink.com/

https://nvd.nist.gov/vuln/detail/CVE-2026-5214	8,8	D-Link	Out-of-bounds Write	D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20260205	https://github.com/wudipjq/my_vuln/blob/main/D-Link8/vuln_169/169.md https://vuldb.com/submit/780439 https://vuldb.com/vuln/354349 https://vuldb.com/vuln/354349/cti https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-5272	8,8	GPU in Google Chrome	Heap-based Buffer Overflow	GPU in Google Chrome prior to 146.0.7680.178	https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html https://issues.chromium.org/issues/491732188
https://nvd.nist.gov/vuln/detail/CVE-2026-5279	8,8	V8 in Google Chrome	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	V8 in Google Chrome prior to 146.0.7680.178	https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html https://issues.chromium.org/issues/490642836
https://nvd.nist.gov/vuln/detail/CVE-2026-5286	8,8	Dawn in Google Chrome	Use after free	Dawn in Google Chrome prior to 146.0.7680.178	https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html https://issues.chromium.org/issues/493900619
https://nvd.nist.gov/vuln/detail/CVE-2026-5287	8,8	PDF in Google Chrome	Use after free	PDF in Google Chrome prior to 146.0.7680.178	https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html https://issues.chromium.org/issues/494644471
https://nvd.nist.gov/vuln/detail/CVE-2026-5292	8,8	WebCodecs in Google Chrome	Out-of-bounds Read	WebCodecs in Google Chrome prior to 146.0.7680.178	https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html https://issues.chromium.org/issues/492213293
https://nvd.nist.gov/vuln/detail/CVE-2026-5349	8,8	Trendnet	Improper Restriction of Operations within the Bounds of a Memory Buffer		https://github.com/panda666-888/vuls/blob/main/trendnet/tew-657brm/add_apcdb.md https://vuldb.com/submit/781563 https://vuldb.com/vuln/354702 https://vuldb.com/vuln/354702/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-5350	8,8	Trendnet	Improper Restriction of Operations within the Bounds of a Memory Buffer	Trendnet TEW-657BRM 1.00.1	https://github.com/panda666-888/vuls/blob/main/trendnet/tew-657brm/update_pcdb.md https://vuldb.com/submit/781567 https://vuldb.com/vuln/354703 https://vuldb.com/vuln/354703/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-5463	8,6	pymetasploit3	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Command injection vulnerability in console.run_module_with_output() in pymetasploit3 through version 1.0.6	https://github.com/DanMcInerney/pymetasploit3 https://pypi.org/project/pymetasploit3/

https://nvd.nist.gov/vuln/detail/CVE-2026-4101	8,1	IBM	Improper Authentication	IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1	https://www.ibm.com/support/pages/node/7268253
https://nvd.nist.gov/vuln/detail/CVE-2026-5282	8,1	WebCodecs in Google Chrome	Out of bounds read	WebCodecs in Google Chrome prior to 146.0.7680.178	https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html https://issues.chromium.org/issues/491655161
https://nvd.nist.gov/vuln/detail/CVE-2026-20155	8,0	Cisco	Missing Authorization	Cisco Evolved Programmable Network Manager (EPNM)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-epnm-improp-auth-mUwFWUU3
https://nvd.nist.gov/vuln/detail/CVE-2026-23407	7,8	Linux kernel		Linux kernel	https://git.kernel.org/stable/c/5a68e46dfe0c8c8ffc6f425ebc4cae6238566ecc https://git.kernel.org/stable/c/76b4d36c5122866452d34d8f79985e191f9c3831 https://git.kernel.org/stable/c/7c7cf05e0606f554c467e3a4dc49e2e578a755b4 https://git.kernel.org/stable/c/d352873bbefa7eb39995239d0b44ccdf8aaa79a4 https://git.kernel.org/stable/c/f39e126e56c6ec1930fae51ad6bca3dae2a4c3ed
https://nvd.nist.gov/vuln/detail/CVE-2026-23411	7,8	Linux kernel		Linux kernel	https://git.kernel.org/stable/c/13bc2772414d68e94e273dea013181a986948ddf https://git.kernel.org/stable/c/2a732ed26fbd048e7925d227af8cf9ea43fb5cc9 https://git.kernel.org/stable/c/8e135b8aee5a06c52a4347a5a6d51223c6f36ba3 https://git.kernel.org/stable/c/ae10787d955fb255d381e0d5589451dd72c614b1 https://git.kernel.org/stable/c/eecce026399917f6efa532c56bc7a3e9dd6ee68b
https://nvd.nist.gov/vuln/detail/CVE-2026-24165	7,8	NVIDIA	Deserialization of Untrusted Data	NVIDIA BioNeMo	https://nvd.nist.gov/vuln/detail/CVE-2026-24165 https://nvidia.custhelp.com/app/answers/detail/a_id/5808 https://www.cve.org/CVERecord?id=CVE-2026-24165
https://nvd.nist.gov/vuln/detail/CVE-2026-24154	7,6	NVIDIA	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	NVIDIA Jetson Linux	https://nvd.nist.gov/vuln/detail/CVE-2026-24154 https://nvidia.custhelp.com/app/answers/detail/a_id/5797 https://www.cve.org/CVERecord?id=CVE-2026-24154
https://nvd.nist.gov/vuln/detail/CVE-2024-44303	7,5	macOS	Improper Access Control	macOS Sequoia 15.1	https://support.apple.com/en-us/121564
https://nvd.nist.gov/vuln/detail/CVE-2025-58136	7,5	Apache Traffic Server	Always-Incorrect Control Flow Implementation	Apache Traffic Server: from 10.0.0 through 10.1.1, from 9.0.0 through 9.2.12	https://lists.apache.org/thread/2s11roxlv1j8ph6q52rqo1klvl01n14q
https://nvd.nist.gov/vuln/detail/CVE-2025-65114	7,5	Apache Traffic Server	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')	This issue affects Apache Traffic Server: from 9.0.0 through 9.2.12, from 10.0.0 through 10.1.1	https://lists.apache.org/thread/2s11roxlv1j8ph6q52rqo1klvl01n14q

https://nvd.nist.gov/vuln/detail/CVE-2026-31937	7,5	Suricata	Inefficient Algorithmic Complexity	Suricata is a network IDS, IPS and NSM engine. Prior to version 7.0.15	https://github.com/OISF/suricata/security/advisories/GHSA-86vg-w8vm-m3gg https://redmine.openinfosecfoundation.org/issues/8304
https://nvd.nist.gov/vuln/detail/CVE-2026-34601	7,5	xmldom	XML Injection (aka Blind XPath Injection)	xmldom is a pure JavaScript W3C standard-based (XML DOM Level 2 Core) `DOMParser` and `XMLSerializer` module. In xmldom versions 0.6.0 and prior and @xmldom/xmldom prior to versions 0.8.12 and 0.9.9, xmldom/xmldom	https://github.com/xmldom/xmldom/commit/2b852e836ab86dbbd6cbaf0537f584dd0b5ac184 https://github.com/xmldom/xmldom/releases/tag/0.8.12 https://github.com/xmldom/xmldom/releases/tag/0.9.9 https://github.com/xmldom/xmldom/security/advisories/GHSA-wh4c-j3r5-mjhp
https://nvd.nist.gov/vuln/detail/CVE-2026-34785	7,5	Rack	Partial String Comparison	Rack is a modular Ruby web server interface. Prior to versions 2.2.23, 3.1.21, and 3.2.6	https://github.com/rack/rack/security/advisories/GHSA-h2jq-g4cq-5ppq
https://nvd.nist.gov/vuln/detail/CVE-2026-35385	7,5	OpenSSH	Improper Preservation of Permissions	OpenSSH before 10.3	https://marc.info/?l=openssh-unix-dev&m=177513443901484&w=2 https://www.openssh.org/releasenotes.html#10.3p1 https://www.openwall.com/lists/oss-security/2026/04/02/3
https://nvd.nist.gov/vuln/detail/CVE-2026-1345	7,3	IBM	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1	https://www.ibm.com/support/pages/node/7268253
https://nvd.nist.gov/vuln/detail/CVE-2026-20151	7,3	Cisco	Insertion of Sensitive Information Into Sent Data	Cisco Smart Software Manager On-Prem (SSM On-Prem)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-priv-esc-xRAnOuO8
https://nvd.nist.gov/vuln/detail/CVE-2026-22768	7,3	Dell	Incorrect Permission Assignment for Critical Resource	Dell AppSync, version(s) 4.6.0	https://www.dell.com/support/kbdoc/en-us/000446965/dsa-2026-163-security-update-for-dell-appsync-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2026-27101	7,2	Dell	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Dell Secure Connect Gateway (SCG) 5.0 Appliance and Application version(s) 5.28.00.xx to 5.32.00.xx	https://www.dell.com/support/kbdoc/en-us/000438589/dsa-2026-020-security-update-for-dell-secure-connect-gateway-application-and-appliance-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2026-34790	7,1	Endian Firewall	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Endian Firewall version 3.3.25 and prior	https://help.endian.com/hc/en-us/sections/360004371358-Community https://www.vulncheck.com/advisories/endian-firewall-cgi-bin-backup-cgi-remove-archive-directory-traversal

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
https://www.cisa.gov/news-events/alerts/2026/04/01/cisa-adds-one-known-exploited-vulnerability-catalog	▪ CVE-2026-5281 Google Dawn Use-After-Free Vulnerability	https://www.cisa.gov/news-events/alerts/2026/04/01/cisa-adds-one-known-exploited-vulnerability-catalog
https://www.cisa.gov/news-events/alerts/2026/04/02/cisa-adds-one-known-exploited-vulnerability-catalog	▪ CVE-2026-3502 TrueConf Client Download of Code Without Integrity Check Vulnerability	https://www.cisa.gov/news-events/alerts/2026/04/02/cisa-adds-one-known-exploited-vulnerability-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
How Elite SOCs Cut Escalation Rates by Arming Tier 1 With Better Threat Intelligence	https://cybersecuritynews.com/reduce-soc-escalation-rates-tier-1-alert-triage/
Qilin Ransomware Uses Malicious DLL to Kill Almost Every Vendor's EDR Solutions	https://cybersecuritynews.com/qilin-ransomware-kill-edr/
OpenSSH 10.3 Fixes Shell Injection and Multiple SSH Security Issues	https://cybersecuritynews.com/openssh-10-3-release/
New ZAP PTK Add-On Maps Browser Security Findings as Native Alert Into ZAP	https://cybersecuritynews.com/zap-ptk-add-on/
WhatsApp Warns Users Targeted by Spyware Attack via Weaponized Version of the App	https://cybersecuritynews.com/whatsapp-warns-users/
Oracle Lays Off 30,000 Employees to Ramp Up Investment in AI Technologies	https://cybersecuritynews.com/oracle-lays-off-30000-employees/
Starbucks Breach – Attacks Allegedly Claim 10GB of Stolen Source Code	https://cybersecuritynews.com/starbucks-breach/
Magecart Hackers Uses 100+ Domains to Hijack eStores Checkouts and Steal Card Data	https://cybersecuritynews.com/magecart-hijack-estore-checkouts/
Google Cloud's Vertex AI platform Vulnerability Allow Attackers to Access Sensitive Data	https://cybersecuritynews.com/google-clouds-vertex-ai-platform-vulnerability/
Russian Hackers Using Remote Access Toolkit "CTRL" for RDP Hijacking	https://cybersecuritynews.com/ctrl-for-rdp-hijacking/
HSBC India Asks Customers to use All-Uppercase Passwords	https://cybersecuritynews.com/hsbc-india-uppercase-passwords/
Windows 11 Emergency Update to Fix Installation Loop Issues	https://cybersecuritynews.com/windows-11-emergency-update/

Google Now Allows You to Change Your @gmail.com Address in a Few Simple Steps	https://cybersecuritynews.com/google-change-gmail-address/
Google Unveils Ransomware Detection and File Restoration for Google Drive	https://cybersecuritynews.com/google-drive-ransomware-detection-2/
Apple New macOS Tahoe Feature Warns Users on ClickFix Attacks	https://cybersecuritynews.com/clickfix-protection-macos-tahoe-26-4/
Microsoft to Remove EXIF Data for Images Shared on Teams	https://cybersecuritynews.com/microsoft-remove-exif-data-teams/

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
CERT-EU Confirms Trivy Supply Chain Attack Led to European Commission AWS Breach	https://cybersecuritynews.com/european-commission-breach-trivy/
Adobe Breach – Threat Actor Allegedly Claims Leak of 13 Million Support Tickets and Employee Records	https://cybersecuritynews.com/adobe-breach/
CareCloud Data Breach – Hackers Accessed IT Infrastructure and Stole Patient Data	https://cybersecuritynews.com/carecloud-data-breach/
Anthropic's Claude Code Source Code Reportedly Leaked Via Their npm Registry	https://cybersecuritynews.com/claude-code-source-code-leaked/
Cisco Source Code and Data Leak Allegedly Claimed by ShinyHunters	https://cybersecuritynews.com/cisco-source-code-and-data-leak/
Mercor AI Confirms Data Breach Following Lapsus$ Claims of 4TB Data Theft	https://cybersecuritynews.com/mercor-ai-data-breach/

Vulnerabilities / Flaws / Zero-day

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

Σύντομη περιγραφή / Τίτλος	URL
CISA Warns of Chrome 0-Day Vulnerability Actively Exploited in Attacks	https://cybersecuritynews.com/chrome-0-day-flaw-exploited/
Apple Expands iOS 18.7.7 Update to More Devices to Shield Users from DarkSword Exploit	https://cybersecuritynews.com/apple-expands-ios-18-7-7-update/
Cisco Smart Software Manager Vulnerability Let Attackers Execute Arbitrary Commands	https://cybersecuritynews.com/cisco-smart-software-manager-vulnerability/
Critical PX4 Autopilot Vulnerability Let Attackers Gain Control Over the Drones	https://cybersecuritynews.com/px4-autopilot-vulnerability/
Symantec DLP Agent Vulnerability Let Attackers Escalate Privileges	https://cybersecuritynews.com/symantec-dlp-agent-vulnerability/
Vim Modeline Bypass Vulnerability Let Attackers Execute Arbitrary OS Commands	https://cybersecuritynews.com/vim-modeline-bypass-vulnerability/
Public PoC Exploit Released for Nginx-UI Backup Restore Vulnerability	https://cybersecuritynews.com/nginx-ui-backup-restore-vulnerability/
Hackers Actively Exploiting Critical WebLogic RCE Vulnerabilities in Attacks	https://cybersecuritynews.com/hackers-exploiting-weblogic-rce-vulnerabilities/
New Chrome Zero-Day Vulnerability Actively Exploited in Attacks — Patch Now	https://cybersecuritynews.com/chrome-zero-day-vulnerability-exploited/
PNG Vulnerabilities Allow Attackers to Trigger Process Crashes, Leak Sensitive Information	https://cybersecuritynews.com/png-vulnerabilities/
WordPress Plugin Vulnerability Exposes Sensitive Data From 800,000+ Sites	https://cybersecuritynews.com/wordpress-plugin-vulnerability-exposes/
ChatGPT Vulnerability Let Attackers Silently Exfiltrate User Prompts and Other Sensitive Data	https://cybersecuritynews.com/chatgpt-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

Potential threats / Threat intelligence

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

Σύντομη περιγραφή / Τίτλος	URL
North Korea-Linked Hackers Compromise Axios npm Package in Major Supply Chain Attack	https://cybersecuritynews.com/north-korea-linked-hackers-compromise-axios-npm-package/
North Korea-Related Campaign Abuses GitHub as C2 in New LNK Phishing Attacks	https://cybersecuritynews.com/north-korea-related-campaign-abuses-github/
Hackers Clone CERT-UA Site to Trick Victims Into Installing Go-Based RAT	https://cybersecuritynews.com/hackers-clone-cert-ua-site/
New Akira Lookalike Ransomware Campaign Targeting Windows Users in South America	https://cybersecuritynews.com/new-akira-lookalike-ransomware-campaign/
Hackers Abuse DOCX, RTF, JS, and Python in Stealthy Boeing RFQ Malware Cam-paign	https://cybersecuritynews.com/hackers-abuse-docx-rtf-js-and-python-in-boeing-rfq/
NoVoice on Google Play with 22 Exploits Attacks Millions of Android Users	https://cybersecuritynews.com/novoice-on-google-play/
Microsoft Details Steps to Mitigate the Axios npm Supply Chain Compromise	https://cybersecuritynews.com/microsoft-details-steps-to-mitigate-the-axios/
FBI Warns of Chinese Mobile Apps May Expose User Data to Cyberattacks	https://cybersecuritynews.com/fbi-warns-of-chinese-mobile-apps/
TA416 Expands Espionage Operations Across Europe With Web Bug Recon and Mal-ware Delivery	https://cybersecuritynews.com/ta416-expands-espionage-operations-across-europe/
New WhatsApp Attack Chain Uses VBS Scripts, Cloud Downloads, and MSI Back-doors	https://cybersecuritynews.com/new-whatsapp-attack-chain-uses-vbs-scripts/
Hackers Use EtherRAT and EtherHiding to Hide Malware Infrastructure on Ethereum	https://cybersecuritynews.com/hackers-use-etherrat-and-etherhiding/
Hackers Push CrystalX Malware-as-a-Service Through Telegram With Stealer and RAT Features	https://cybersecuritynews.com/hackers-push-crystalx-malware-as-a-service/
Hackers Hijack Hotel Booking Workflows to Scam Guests With Fake Payment Re-quests	https://cybersecuritynews.com/hackers-hijack-hotel-booking-workflows/
North Korean Hackers Compromise Popular Axios Package to Infect Windows, ma-cOS, and Linux	https://cybersecuritynews.com/north-korean-hackers-compromise-widely-used-axios-package/
Hackers Backdoor Telnyx Python SDK on PyPI to Steal Credentials Across Windows, macOS, and Linux	https://cybersecuritynews.com/hackers-backdoor-telnyx-python-sdk-on-pypi/
New npm Supply Chain Attack Uses undicy-http to Deploy Screen-Streaming RAT and Browser Injector	https://cybersecuritynews.com/new-npm-supply-chain-attack-uses-undicy-http/
XLoader Malware Upgrades Obfuscation Tactics and Hides C2 Traffic Behind Decoy Servers	https://cybersecuritynews.com/xloader-malware-upgrades-obfuscation-tactics/
Hackers Weaponize Legitimate Windows Tools to Disable Antivirus Before Ransom-ware Attacks	https://cybersecuritynews.com/hackers-weaponize-legitimate-windows-tools/
Hackers Deploy Telegram-Based ResokerRAT With Screenshot and Persistence Fea-tures	https://cybersecuritynews.com/hackers-deploy-telegram-based-resokerrat/
EvilTokens Emerges as New Phishing-as-a-Service Platform for Microsoft Account Takeover	https://cybersecuritynews.com/eviltokens-emerges-as-new-phishing-as-a-service-platform/
Remcos RAT Infection Chain Hides Behind Obfuscated Scripts and Trusted Windows Binaries	https://cybersecuritynews.com/remcos-rat-infection-chain-hides-behind-obfuscated/

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
20 Best Application Performance Monitoring Tools in 2026	https://cybersecuritynews.com/application-performance-monitoring-tools/
Best VPN For Linux In 2026	https://cybersecuritynews.com/best-vpn-for-linux/
10 Best VPN For Privacy In 2026	https://cybersecuritynews.com/best-vpn-for-privacy/
Top 20 Best Digital Forensic Tools in 2026	https://cybersecuritynews.com/best-digital-forensic-tools/

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 CVSSv3 score >= 7.0 και έχει γίνει μια επιλογή συστημάτων/υπηρεσιών ανάλογα με το πόσο διαδεδομένα είναι.

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/