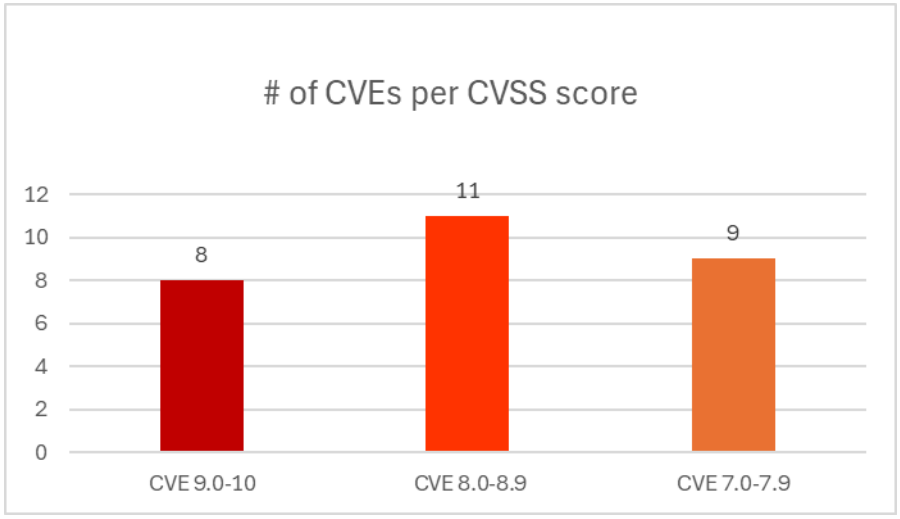
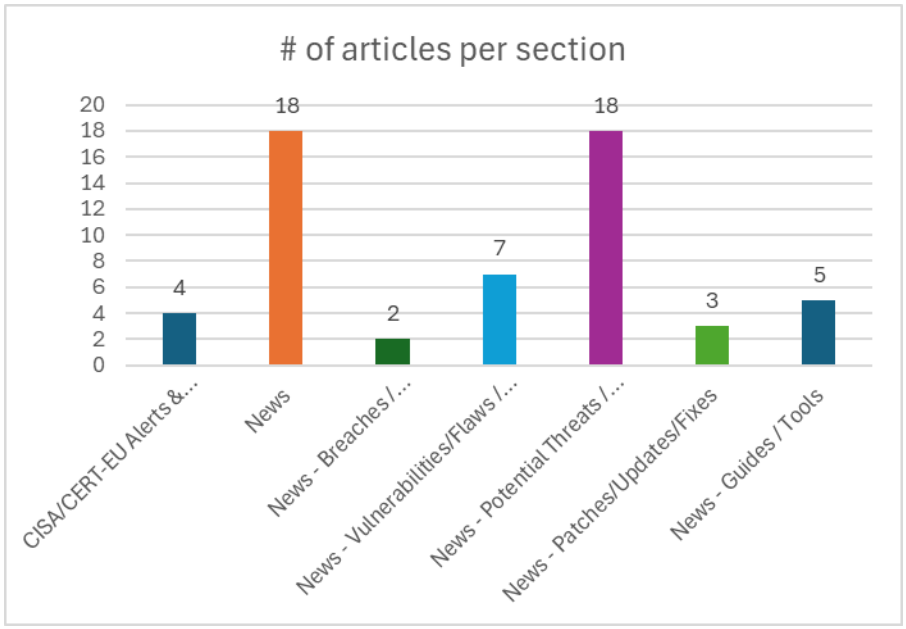


Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 04/11/2026 - 06/11/2026





Contents

Common Vulnerabilities and Exposures (CVEs) 3
CISA/CERT-EU Alerts & Advisories 7
News 8
Breaches / Compromised / Hacked 9
Vulnerabilities / Flaws / Zero-day 10
Patches / Updates / Fixes 10
Potential threats / Threat intelligence 11
Guides / Tools 12
References 13
Annex – Websites with vendor specific vulnerabilities 14

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	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/cve-2026-122006	9,8	The activestorage gem before 8.1.4.1 for Ruby on Rails	Insecure Default Initialization of Resource	The activestorage gem before 8.1.4.1 for Ruby on Rails, when ImageMagick attachment processing occurs, can allow server read and write operations	https://github.com/alan-turing-institute/cyber-threat-observatory/blob/main/reports/2026-11-04/TIER_2_CVE-2026-122006.md https://github.com/digitalocean/droplet-1-clicks/pull/488 https://github.com/rails/rails/releases/tag/v8.0.5.2 https://github.com/rails/rails/releases/tag/v8.1.4.1 https://github.com/rails/rails/security/advisories/GHSA-f3w6-w445-fwh9 https://github.com/rubysec/ruby-advisory-db/pull/1300
https://nvd.nist.gov/vuln/detail/cve-2026-82418	9,8	IBM Watson Speech Services Cartridge	Use After Free	IBM Watson Speech Services Cartridge 4.0.0 through 5.4.0	https://www.ibm.com/support/pages/node/7293510
https://nvd.nist.gov/vuln/detail/cve-2026-83542	9,8	Apache OFBiz	Improper Control of Generation of Code ('Code Injection')	Apache OFBiz 24.09 before 24.09.08	https://lists.apache.org/thread.html/7b2syzksp7klt9fvhdg0olldvs2g83lz
https://nvd.nist.gov/vuln/detail/cve-2026-122311	9,4	Kyverno	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Kyverno from 1.16.0 before 1.19.2	https://github.com/kyverno/kyverno/security/advisories/GHSA-4pqm-wqq6-h9q2 https://www.vulncheck.com/advisories/kyverno-1.16.0-before-1.19.2-path-traversal-in-namespaced-cel-policies-via-resource-argument
https://nvd.nist.gov/vuln/detail/cve-2026-121933	9,3	Linksys	Improper Authentication	Linksys E5350 1.0.00.037	https://github.com/Zimo-666/E5350-cves/tree/main/02-empty-admin-password-auth-bypass https://vuldb.com/cve/CVE-2026-121933 https://vuldb.com/submit/1024276 https://vuldb.com/vuln/431045 https://vuldb.com/vuln/431045/cti https://www.linksys.com/
https://nvd.nist.gov/vuln/detail/cve-2026-122013	9,3	Comfast	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Comfast CF-WR632AX 2.6.0.1	https://github.com/FoundTL/COMFAST-CF-WR632AX-Wi-Fi-6-Router https://vuldb.com/cve/CVE-2026-122013 https://vuldb.com/submit/1023251 https://vuldb.com/vuln/431080 https://vuldb.com/vuln/431080/cti

https://nvd.nist.gov/vuln/detail/cve-2026-122051	9,3	Edimax BR-6208AC 1.32	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	Edimax BR-6208AC 1.32	https://github.com/fizz-is-on-the-way/Iot_vuls/tree/main/BR-6208AC/RCE_mp https://vuldb.com/cve/CVE-2026-122051 https://vuldb.com/submit/1025459 https://vuldb.com/vuln/431135 https://vuldb.com/vuln/431135/cti
https://nvd.nist.gov/vuln/detail/cve-2026-116790	9,1	FreeSWITCH	Authentication Bypass by Spoofing	Prior to 1.11.2	https://github.com/signalwire/freeswitch/commit/68ec688eb601767a28854e804a0e4df5872f5bc7 https://github.com/signalwire/freeswitch/releases/tag/v1.11.2 https://github.com/signalwire/freeswitch/security/advisories/GHSA-rc25-33hp-6mv2
https://nvd.nist.gov/vuln/detail/cve-2026-121065	8,8	Google Chrome	Incorrect Authorization	Incorrect authorization in DevTools in Google Chrome prior to 157.0.8103.38	https://chromereleases.google-blog.com/2026/11/stable-channel-update-for-desktop.html https://issues.chromium.org/issues/562233597
https://nvd.nist.gov/vuln/detail/cve-2026-121068	8,8	Google Chrome	Access of Resource Using Incompatible Type ('Type Confusion')	Type confusion in V8 in Google Chrome prior to 157.0.8103.38	https://chromereleases.google-blog.com/2026/11/stable-channel-update-for-desktop.html https://issues.chromium.org/issues/577327383
https://nvd.nist.gov/vuln/detail/cve-2026-121069	8,8	Google Chrome	Use After Free	Use after free in Track in Google Chrome prior to 157.0.8103.38	https://chromereleases.google-blog.com/2026/11/stable-channel-update-for-desktop.html https://issues.chromium.org/issues/568371493
https://nvd.nist.gov/vuln/detail/cve-2026-121956	8,7	FreeRDP	Double Free	FreeRDP before 3.32.2	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-2557-79qc-6gfr https://www.vulncheck.com/advisories/freerdp-before-3.32.2-double-free-in-winpr-kerberos-retrievesometgt
https://nvd.nist.gov/vuln/detail/cve-2026-121964	8,7	FreeRDP	Heap-based Buffer Overflow	FreeRDP before 3.32.2	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-q82v-5wjg-6h57 https://www.vulncheck.com/advisories/freerdp-before-3.32.2-heap-buffer-overflow-via-rpc-client-recv-fragment
https://nvd.nist.gov/vuln/detail/cve-2026-119742	8,6	Nagios XI	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Nagios XI before 2026R2	https://www.nagios.com/security-disclosures/nagios-xi/2026r2/ https://www.vulncheck.com/advisories/nagios-xi-2026r2-os-command-injection-via-mibs-php
https://nvd.nist.gov/vuln/detail/cve-2026-82033	8,6	DeepSeek Harness	Missing Authentication for Critical Function	DeepSeek Harness prior to 0.1.2-alpha.2, and specifically commit 3e24087	https://github.com/deepseek-ai/deepseek-harness/commit/3e24087bfaeabe40b58ba2f7b936895b8f93fe27 https://github.com/deepseek-ai/deepseek-harness/releases/tag/dsh-v0.1.2-alpha.2 https://www.vulncheck.com/advisories/deepseek-harness-unauthenticated-rpc-command-execution

https://nvd.nist.gov/vuln/detail/cve-2026-11724	**8,5**	IBM MQ	Improper Input Validation	IBM MQ 9.2.0.0 through 9.2.0.44 LTS, 9.3.0.0 through 9.3.0.42 LTS, 9.4.0.0 through 9.4.0.26 LTS, 9.4.0.0 through 9.4.5.1 CD, and 10.0.0.0 through 10.0.0.5 LTS and CD	https://www.ibm.com/support/pages/node/7294503
https://nvd.nist.gov/vuln/detail/cve-2026-121931	**8,5**	Linksys	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Linksys WRT54GL 4.30.18	https://github.com/Zimo-666/WRT54GL-cves/tree/main/CVE-TBD-traceroute-ip-command-injection https://vuldb.com/cve/CVE-2026-121931 https://vuldb.com/submit/1024099 https://vuldb.com/vuln/431043 https://vuldb.com/vuln/431043/cti https://www.linksys.com/
https://nvd.nist.gov/vuln/detail/cve-2026-92698	**8,2**	FastNetMon	Out-of-bounds Read	FastNetMon is a high-performance DDoS detector and sensor. In version 1.2.9 and earlier	https://github.com/pavel-odintsov/fastnetmon/commit/6871b7383322db14405a8de1399a83da15ef3533 https://github.com/pavel-odintsov/fastnetmon/commit/be81c403b9aa891f8444a6379cd4a4fbbc324a83 https://github.com/pavel-odintsov/fastnetmon/pull/1089 https://github.com/pavel-odintsov/fastnetmon/pull/1093 https://github.com/pavel-odintsov/fastnetmon/security/advisories/GHSA-852r-3wcv-pjx2
https://nvd.nist.gov/vuln/detail/cve-2026-102523	**8,0**	MariaDB	External Control of File Name or Path	rom 10.11.1 until 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2	https://github.com/MariaDB/server/commit/98437c30ae52ed709f266e5f8095d779261a5879 https://github.com/MariaDB/server/releases/tag/mariadb-10.11.19 https://github.com/MariaDB/server/releases/tag/mariadb-11.4.13 https://github.com/MariaDB/server/releases/tag/mariadb-11.8.9 https://github.com/MariaDB/server/releases/tag/mariadb-12.3.3 https://github.com/MariaDB/server/releases/tag/mariadb-13.0.2 https://github.com/MariaDB/server/security/advisories/GHSA-h4vr-wpff-jfx4 https://jira.mariadb.org/browse/MDEV-40413
https://nvd.nist.gov/vuln/detail/cve-2026-59264	**7,8**	The Windows installers of Apache OpenOffice	Uncontrolled Search Path Element	The Windows installers of Apache OpenOffice 4.1.16	http://www.openwall.com/lists/oss-security/2026/11/03/22 https://lists.apache.org/thread.html/d4n33sjk8jgrr78jj5cq5r51fvxv6nnv

https://nvd.nist.gov/vuln/detail/cve-2026-123059	**7,5**	Eclipse BaSyx Helm Charts	Cleartext Storage of Sensitive Information	Eclipse BaSyx Helm Charts version 2.2.0	https://github.com/eclipse-basyx/charts/pull/46 https://github.com/eclipse-basyx/charts/releases/tag/aas-basyx-v2-full-2.2.0 https://github.com/eclipse-basyx/charts/security/advisories/GHSA-6438-759f-6f8v https://gitlab.eclipse.org/security/cve-assignment/-/work_items/546
https://nvd.nist.gov/vuln/detail/cve-2026-17493	**7,5**	IBM MQ	Improper Restriction of XML External Entity Reference	IBM MQ 9.2.0.0 through 9.2.0.44 LTS, 9.3.0.0 through 9.3.0.42 LTS, 9.4.0.0 through 9.4.0.26 LTS, 9.4.0.0 through 9.4.5.1 CD, and 10.0.0.0 through 10.0.0.5 LTS and CD	https://www.ibm.com/support/pages/node/7294499
https://nvd.nist.gov/vuln/detail/cve-2026-63655	**7,5**	tsParticles	Uncontrolled Resource Consumption	sParticles is a TypeScript library for creating highly customizable particle animations. Prior to 4.3.1	https://github.com/tsparticles/tsparticles/commit/25fb70e7f527a91568adaef576570289083f243b https://github.com/tsparticles/tsparticles/commit/7b3a9488d4201fe9ddd5fec05f4a2ae65d3627ea https://github.com/tsparticles/tsparticles/pull/5875 https://github.com/tsparticles/tsparticles/releases/tag/v4.3.1 https://github.com/tsparticles/tsparticles/security/advisories/GHSA-447x-qqwf-m7xq
https://nvd.nist.gov/vuln/detail/cve-2026-82904	**7,5**	Apache OFBiz	Allocation of Resources Without Limits or Throttling	Apache OFBiz 24.09 before 24.09.08	https://lists.apache.org/thread.html/7b2syzksp7klt9fvhdg0olldvs2g83lz
https://nvd.nist.gov/vuln/detail/cve-2026-97705	**7,5**	Moleculer	Loop with Unreachable Exit Condition ('Infinite Loop')	Moleculer is a progressive microservices framework for Node.js. Prior to 0.14.36 and 0.15.2	https://github.com/moleculerjs/moleculer/commit/168ec-bdc245c9a9d1dc4ef9b8a81dbae38ee3063 https://github.com/moleculerjs/moleculer/commit/914074e502ae403a0338ad168b45b16d6bcc3e44 https://github.com/moleculerjs/moleculer/releases/tag/v0.14.36 https://github.com/moleculerjs/moleculer/releases/tag/v0.15.2 https://github.com/moleculerjs/moleculer/security/advisories/GHSA-h89v-g948-47vp
https://nvd.nist.gov/vuln/detail/cve-2026-116789	**7,4**	FreeSWITCH	Improper Certificate Validation	Prior to 1.11.2	https://github.com/signalwire/freeswitch/commit/ea74c0acb8b85c5fc50158cd592a1b80c4edf6a6 https://github.com/signalwire/freeswitch/releases/tag/v1.11.2 https://github.com/signalwire/freeswitch/security/advisories/GHSA-8ghv-ccjr-4cx9
https://nvd.nist.gov/vuln/detail/cve-2026-90634	**7,3**	Apache OpenOffice	Out-of-bounds Write	Apache OpenOffice versions through 4.1.16	http://www.openwall.com/lists/oss-security/2026/11/03/32 https://lists.apache.org/thread.html/1c0lropx46w8ozwk29p5yw1xlq4wnbll

https://nvd.nist.gov/vuln/detail/cve-2026-120956	**7,1**	MongoDB C Driver	Reachable Assertion	-	https://jira.mongodb.org/browse/CDRIVER-6501

CISA/CERT-EU Alerts & Advisories

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

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2026-119977 WordPress Core Time-of-check Time-of-use (TOCTOU) Race Condition Vulnerability	https://www.cisa.gov/news-events/alerts/2026/11/03/cisa-adds-one-known-exploited-vulnerability-catalog
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2024-27834 Apple Multiple Products Improper Authentication Vulnerability	https://www.cisa.gov/news-events/alerts/2026/11/04/cisa-adds-one-known-exploited-vulnerability-catalog
US Government Partners Urge Hardening Industrial Refrigeration and Cold Chain Monitoring Systems		https://www.cisa.gov/resources-tools/resources/us-government-partners-urge-hardening-industrial-refrigeration-and-cold-chain-monitoring-systems
Post-Quantum Questions to Ask Your Vendors		https://www.cisa.gov/resources-tools/resources/post-quantum-questions-ask-your-vendors

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
ARTEX AI Hacking Framework Found on 1,465 Public Servers, Some Hosting Cyberattack Tools	https://cybersecuritynews.com/artex-ai-hacking-framework/
OpenAI Launches GPT-6 Cyber That Finds 81 Firefox Flaws and Develops 948 Linux Exploits	https://cybersecuritynews.com/openai-launches-gpt-6-cyber/
Shopify Mandates IP Allowlisting for Public Apps to Prevent Unauthorized Admin API Access	https://cybersecuritynews.com/shopify-mandates-ip-allowlisting/
ARTEX Hackers Expose Their Own Servers, Revealing AI Tools Behind South Korean Bank Breaches	https://cybersecuritynews.com/artex-hackers/
One Hacker Uses 12 AI Agents to Breach Taiwan's Emergency Services and Steal Sensitive Data	https://cybersecuritynews.com/one-hacker-uses-12-ai-agents/
Apple to Scan for Every Photo and File Shared Through a Public iCloud Link for Harmful Content	https://cybersecuritynews.com/apple-to-scan-for-every-photo-and-file/
SkyW4lker Phishing Campaign Expands, Threatening US Enterprises with Microsoft 365 Account Takeovers	https://cybersecuritynews.com/skyw4lker-phishing-campaign-expands-threatening-us-enterprises-with-microsoft-365-account-takeovers/
6 Challenges SOC Leaders Should Turn into Priorities in 2027	https://cybersecuritynews.com/6-challenges-soc-leaders-should-turn-into-priorities-in-2027/
French Bank Crédit Mutuel Arkéa Confirms Cyberattack Amid Reports of $133 Million Theft	https://cybersecuritynews.com/credit-mutuel-arkea-confirms-cyberattack/
Microsoft Edge Now Automatically Blocks Malicious Websites Sending Fake Virus Alert Notifications	https://cybersecuritynews.com/microsoft-edge/
Cloudflare Launches Zero Wire to Track Critical CVEs, Active Exploits, and Security Fixes	https://cybersecuritynews.com/cloudflare-launches-zero-wire/
Ransomware Gangs Claim 30% More Victims, but Researchers Warn Some Breaches May Be Fake	https://cybersecuritynews.com/ransomware-gangs/
Hackers Use Stolen Microsoft Entra ID and Azure DevOps Credentials to Access 27 Organizations	https://cybersecuritynews.com/stolen-entra-id-and-azure-credentials/

Σύντομη περιγραφή / Τίτλος	URL
Hackers Use OpenAI Codex Jailbreak Toolkit That Secretly Injects Ads Into AI Responses	https://cybersecuritynews.com/openai-codex-jailbreak/
Hackers Launch LLMHijacking Attacks, Leaving Companies With $1 Million in Cloud Bills	https://cybersecuritynews.com/llmhijacking-attacks/
Hackers Hijacked French Blood Plasma Freezers, Changing Temperature Settings From −30°C to 110°C	https://cybersecuritynews.com/french-blood-plasma-freezers-hacked/
OpenAI Builds Pando Git Infrastructure Using AI Agents and Deploys Continuous Security Testing	https://cybersecuritynews.com/openai-builds-pando-git-infrastructure/
North Korean Hackers Abuse Internal AI Tool and Fake Job Interviews in $6.34 Billion Binance Heist	https://cybersecuritynews.com/fake-job-interviews-binance-heist/

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
DigiCert Confirms Data Breach Exposing Customer Details and Sensitive Identity Documents	https://cybersecuritynews.com/digicert-confirms-data-breach/
DreamHost Confirms Data Breach – Hackers Stole Customer Credentials and Accessed Emails	https://cybersecuritynews.com/dreamhost-confirms-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
Microsoft Paint 0-Click Vulnerability Could Allow Hackers to Take Control of Windows PCs	https://cybersecuritynews.com/windows-paint-rce-vulnerability/
Critical Citrix XenServer Vulnerability Could Let Hackers Take Over Virtualization Hosts Without Authentication	https://cybersecuritynews.com/critical-citrix-xenserver-vulnerability/
OpenAI Cyber Model Uncovers 948 Linux Kernel Privilege Escalation Vulnerabilities	https://cybersecuritynews.com/openai-uncovers-948-linux-kernel-vulnerabilities/
Critical Ruby on Rails Flaw Could Let Hackers Steal Server Secrets Through Malicious Image Uploads	https://cybersecuritynews.com/critical-ruby-on-rails-flaw/
Gorbag Hackers Exploit WinRAR Vulnerability to Steal Credentials From Ukrainian Government Agencies	https://cybersecuritynews.com/gorbag-hackers-exploit-winrar-vulnerability/
Hackers Exploit Zyxel GS1900 Zero-Day in the Wild to Hijack Network Switches	https://cybersecuritynews.com/zyxel-gs1900-zero-day-exploited/
CISA Warns of WordPress Core Vulnerability Exploited in Attacks to Execute Malicious Code	https://cybersecuritynews.com/wordpress-core-vulnerability-exploited/

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
Node.js Schedules High-Severity Security Fixes for 22.x, 24.x, and 26.x Release Lines	https://cybersecuritynews.com/node-js-schedules-patch/
Google Releases Major Chrome Security Update Fixing 213 Bugs, Including 7 Critical Vulnerabilities	https://cybersecuritynews.com/google-releases-major-chrome-security-update/
Google Patches Over 200 Android Vulnerabilities, Including Critical Zero-Click RCE Flaws	https://cybersecuritynews.com/android-0-click-remote-code-execution-flaws/

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
Claude Dispatch Flaw Lets Malicious Browser Extensions Run Code on Connected Computers	https://cybersecuritynews.com/claude-dispatch-vulnerability/
Hackers Could Bypass ChatGPT Lockdown Mode to Steal Con-versations Without Users Knowing	https://cybersecuritynews.com/chatgpt-lockdown-mode-bypass/
GhostMap Android Flaw Can Trap Phones in Endless Reboot Loops Without Opening an App	https://cybersecuritynews.com/ghostmap-android-vulnerability/
Hackers Turn Popular Chinese Keyboard Software Into a Backdoor for Cyberespionage Attacks	https://cybersecuritynews.com/chinese-keyboard-software/
OpenSSH Flaw Could Let Attackers Bypass Password Authen-tication on Alpine Linux Servers	https://cybersecuritynews.com/openssh-flaw-bypass-password-authentication/
HYFLOCK Ransomware Encrypts Only First 4KB of Larger Files, Leaves Parts of Victims' Files Accessible	https://cybersecuritynews.com/hyflock-ransomware/
Hackers Hide Marsalek Malware in Fake Roblox and Fortnite Cheats to Steal Passwords and Crypto Wallet Data	https://cybersecuritynews.com/hackers-hide-marsalek-malware/
Tata Motors iRA App Flaws Could Let Hackers Impersonate Car Owners and Access Vehicle Services	https://cybersecuritynews.com/tata-motors-ira-app-flaws/
Hackers Trick Mac Users Into Running Terminal Commands That Install Phexia Password-Stealing Malware	https://cybersecuritynews.com/hackers-trick-mac-users/
Hackers Use Fake Government Websites and CAPTCHA Checks to Deliver SimpleHelp Remote Access Software	https://cybersecuritynews.com/hackers-use-fake-government-websites/
Debian and Ubuntu APT Flaw Lets Hackers Hijack Software Updates and Execute Code as Root	https://cybersecuritynews.com/debian-apt-flaw-lets-hackers-hijack-updates/
Scammers Use Microsoft Azure to Host Fake Windows Secu-rity Alerts Seen at 80 Organizations	https://cybersecuritynews.com/scammers-use-microsoft-azure/
Critical SolarWinds Dameware Flaw Could Allow Attackers to Compromise Remote Systems	https://cybersecuritynews.com/critical-solarwinds-dameware-flaw/
Critical Barracuda Security Flaws Could Let Hackers Bypass Authentication and Gain Root Access	https://cybersecuritynews.com/critical-barracuda-security-flaws/

Σύντομη περιγραφή / Τίτλος	URL
Russian APT29 Hackers Turn Trusted Websites Into Traps to Compromise iPhone and Android Users	https://cybersecuritynews.com/russian-apt29-hackers/
Hackers Hide XLoader Malware in Fake Business Orders to Steal Passwords and Evade Detection	https://cybersecuritynews.com/hackers-hide-xloader-malware/
Hackers Use New Infostealer Malware to Steal ChatGPT, Claude, and Codex Tokens That Survive Password Resets	https://cybersecuritynews.com/hackers-use-new-infostealer-malware/
Hackers Use Fake Software Downloads to Secretly Hijack Windows PCs and Monetize Their Resources	https://cybersecuritynews.com/hackers-use-fake-software-downloads/

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
Top 10 Best Deception Technology Solutions in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-deception-technology/
Top 10 Best Security Data Lake Platforms in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-security-data-lakes/
Top 10 Best Security Log Management Tools in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-security-log-management/
Top 10 Best Threat Hunting Services in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-threat-hunting-services/
Top 10 Best Breach & Attack Simulation (BAS) Tools in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-bas-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 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/