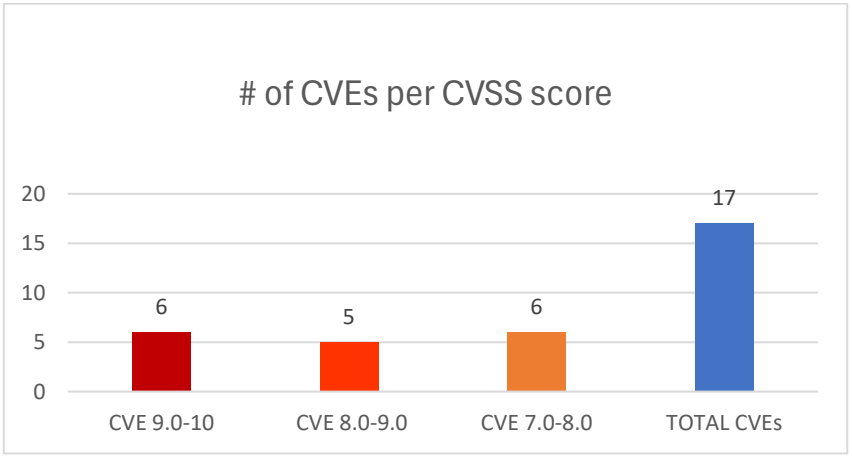
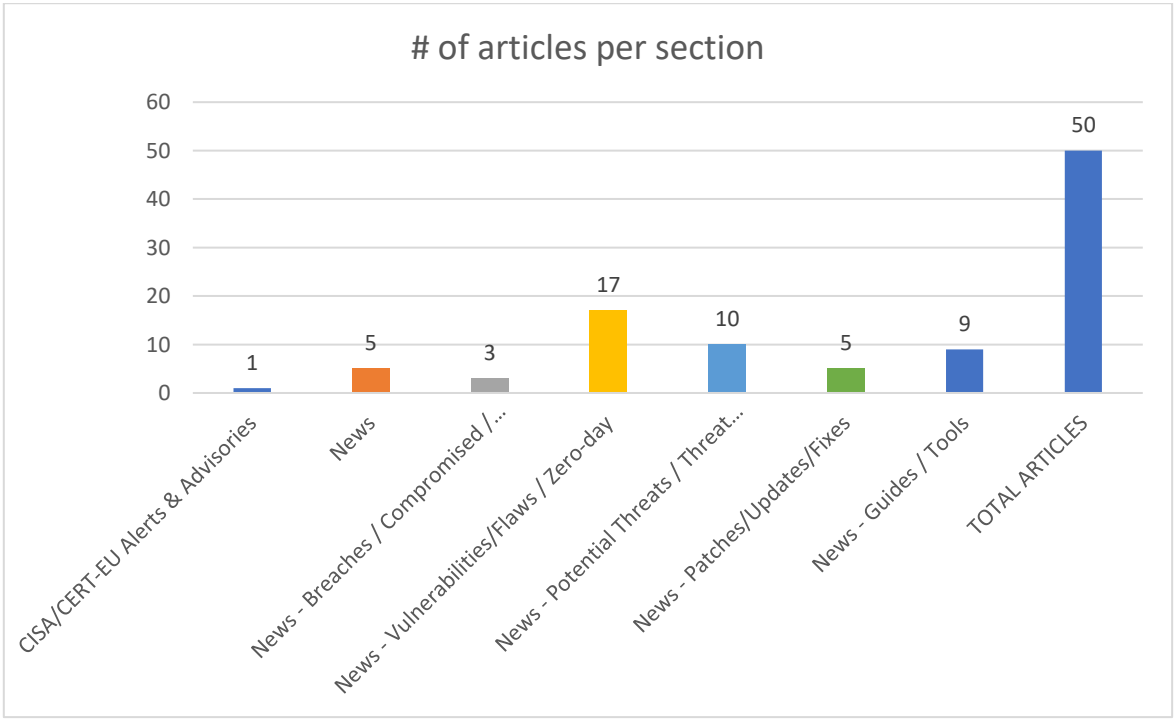
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 18/02/2026 - 20/02/2026





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-2026-27180	9.8	MajorDoMo	Download of Code Without Integrity Check		https://chocapikk.com/posts/2026/majordomo-revisited/ VulnCheck https://github.com/sergejey/majordomo/pull/1177 VulnCheck https://www.vulncheck.com/advisories/majordomo-supply-chain-remote-code-execution-via-update-url-poisoning
https://nvd.nist.gov/vuln/detail/CVE-2026-2686	9.8	SECCN Dingcheng	Improper Neutralization of Special Elements used in a Command ('Command Injection')	G10 3.1.0.181203	https://github.com/cha0yang1/SECCN/blob/main/UnauthorizedRCE.md VulDB https://github.com/cha0yang1/SECCN/blob/main/UnauthorizedRCE.md#2-vulnerability-reproduction-proof-of-concept VulDB https://vuldb.com/?ctiid.346488 VulDB https://vuldb.com/?id.346488 VulDB https://vuldb.com/?submit.754200
https://nvd.nist.gov/vuln/detail/CVE-2026-27476	9.8	RustFly	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	2.0.0	https://packetstorm.news/files/id/215819/ VulnCheck https://www.vulncheck.com/advisories/rustfly-command-injection-via-udp-remote-control
https://nvd.nist.gov/vuln/detail/CVE-2026-26339	9.8	Hyland Alfresco Transformation Service	Server-Side Request Forgery (SSRF)	-	https://www.hyland.com/en/solutions/products/alfresco-platform VulnCheck https://www.vulncheck.com/advisories/hyland-alfresco-transformation-service-argument-injection-rce
https://nvd.nist.gov/vuln/detail/CVE-2026-26980	9.4	Ghost	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Versions 3.24.0 through 6.19.0	https://github.com/TryGhost/Ghost/commit/30868d632b2252b638bc8a4c8ebf73964592ed91 GitHub, Inc. https://github.com/TryGhost/Ghost/releases/tag/v6.19.1 GitHub, Inc. https://github.com/TryGhost/Ghost/security/advisories/GHSA-w52v-v783-gw97
https://nvd.nist.gov/vuln/detail/CVE-2026-25548	9.1	InvoicePlane	Improper Control of Generation of Code ('Code Injection')	1.7.0	https://github.com/InvoicePlane/InvoicePlane/commit/93622f2df88a860d89bfee56012cabb2942061d6 GitHub, Inc. https://github.com/InvoicePlane/InvoicePlane/security/advisories/GHSA-g6rw-m9mf-33ch

https://nvd.nist.gov/vuln/detail/CVE-2026-26990	8.8	LibreNMS	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Versions 25.12.0 and below	https://github.com/librenms/librenms/commit/15429580baba03ed1dd377bada1bde4b7a1175a1 GitHub, Inc. https://github.com/librenms/librenms/pull/18777 GitHub, Inc. https://github.com/librenms/librenms/security/advisories/GHSA-79q9-wc6p-cf92
https://nvd.nist.gov/vuln/detail/CVE-2026-2649	8.8	Google Chrome	External Control of Assumed-Immutable Web Parameter	prior to 145.0.7632.109	https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_18.html Chrome Release Notes https://issues.chromium.org/issues/481074858
https://nvd.nist.gov/vuln/detail/CVE-2026-27182	8.4	Saturn Remote Mouse Server	Missing Authentication for Critical Function		https://packetstorm.news/files/id/215835/ VulnCheck https://www.saturnremote.com/ VulnCheck https://www.vulncheck.com/advisories/saturn-remote-mouse-server-udp-command-injection-rce
https://nvd.nist.gov/vuln/detail/CVE-2026-27475	8.1	SPIP		before 4.4.9	https://blog.spip.net/Mise-a-jour-de-securite-sortie-de-SPIP-4-4-9.html VulnCheck https://git.spip.net/spip/spip VulnCheck https://www.vulncheck.com/advisories/spip-insecure-deserialization
https://nvd.nist.gov/vuln/detail/CVE-2026-25755	8.1	jsPDF	Improper Control of Generation of Code ('Code Injection')	Prior to 4.2.0	https://github.com/ZeroXJacks/CVEs/blob/main/2026/CVE-2026-25755.md GitHub, Inc. https://github.com/parallax/jsPDF/commit/56b46d45b052346f5995b005a34af5dcdddd5437 GitHub, Inc. https://github.com/parallax/jsPDF/releases/tag/v4.2.0 GitHub, Inc. https://github.com/parallax/jsPDF/security/advisories/GHSA-9vjf-qc39-jprp
https://nvd.nist.gov/vuln/detail/CVE-2026-2576	7.5	The Business Directory Plugin – Easy Listing Directories for WordPress plugin	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to, and including, 6.4.2	https://plugins.trac.wordpress.org/browser/business-directory-plugin/tags/6.4.21/includes/controllers/pages/class-checkout.php#L126 Wordfence https://plugins.trac.wordpress.org/browser/business-directory-plugin/tags/6.4.21/includes/db/class-db-query-set.php#L37 Wordfence https://plugins.trac.wordpress.org/changeset/3463307/business-directory-plugin/trunk/includes/db/class-db-query-set.php Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/d8ec7d25-1574-416c-b5fd-3a71b1cc09d2?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2026-25474	7.5	OpenClaw	Insufficient Verification of Data Authenticity	In versions 2026.1.30 and below	https://github.com/openclaw/openclaw/commit/3cbcba10cf30c2ffb898f0d8c7dfb929f15f8930 GitHub, Inc. Patch https://github.com/openclaw/openclaw/commit/5643a934799dc523ec2ef18c007e1aa2c386b670 GitHub, Inc. Patch https://github.com/openclaw/openclaw/commit/633fe8b9c17f02fcc68ecdb5ec212a5ace932f09 GitHub, Inc. Patch https://github.com/openclaw/openclaw/commit/ca92597e1f9593236ad86810b66633144b69314d GitHub, Inc. Patch https://github.com/openclaw/openclaw/releases/tag/v2026.2.1 GitHub, Inc. Product Release Notes https://github.com/openclaw/openclaw/security/advisories/GHSA-mp5h-m6qj-6292
https://nvd.nist.gov/vuln/detail/CVE-2026-2668	7.3	Rongzhitong Visual Integrated Command and Dispatch Platform	Incorrect Privilege Assignment	up to 20260206	https://github.com/21151213732/CVE/blob/main/VICDP-Unauthorized%20Access2.md VulDB https://vuldb.com/?ctiid.346465 VulDB https://vuldb.com/?id.346465 VulDB https://vuldb.com/?submit.753283
https://nvd.nist.gov/vuln/detail/CVE-2026-2684	7.3	Tsinghua Unigroup Electronic Archives System	Improper Access Control	up to 3.2.210802(62532)	https://github.com/luoye197-prog/ziguang-fileupload VulDB https://github.com/luoye197-prog/ziguang-fileupload/blob/main/introduce%26poc VulDB https://vuldb.com/?ctiid.346475 VulDB https://vuldb.com/?id.346475 VulDB https://vuldb.com/?submit.753973
https://nvd.nist.gov/vuln/detail/CVE-2026-2821	7.3	Fujian Smart Integrated Management Platform System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to 7.5	https://github.com/luoye197-prog/cve-yinda-sql2/blob/main/introduce VulDB https://github.com/luoye197-prog/cve-yinda-sql2/blob/main/poc.py VulDB https://vuldb.com/?ctiid.346946 VulDB https://vuldb.com/?id.346946 VulDB https://vuldb.com/?submit.753405
https://nvd.nist.gov/vuln/detail/CVE-2026-2670	7.2	Advantech WISE-6610 1.2.1_20251110	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Advantech WISE-6610 1.2.1_20251110	https://github.com/master-abc/cve/issues/37 VulDB https://vuldb.com/?ctiid.346467 VulDB https://vuldb.com/?id.346467 VulDB https://vuldb.com/?submit.753293 VulDB https://www.advantech.com/

CISA/CERT-EU Alerts & Advisories

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

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds Two Known Exploited Vulnerabilities to Catalog	▪ CVE-2021-22175 **GitLab Server-Side Request Forgery (SSRF) Vulnerability** ▪ CVE-2026-22769 **Dell RecoverPoint for Virtual Machines (RP4VMs) Use of Hard-coded Credentials Vulnerability**	https://www.cisa.gov/news-events/alerts/2026/02/18/cisa-adds-two-known-exploited-vulnerabilities-catalog

News

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

Σύντομη περιγραφή / Τίτλος	URL
Scam Abuses Gemini Chatbots to Convince People to Buy Fake Crypto	https://www.darkreading.com/endpoint-security/scam-abuses-gemini-chatbots-convince-people-buy-fake-crypto
Record Number of Ransomware Victims and Groups in 2025	https://www.infosecurity-magazine.com/news/record-number-ransomware-victims/
Guardian AI-Penetration Testing Tool Connects Gemini, GPT-4 with 19 Security Tools Including Nmap	https://cybersecuritynews.com/guardian-ai-penetration-testing-tool/
Paloalto to Acquire Koi Security for Establishing Agentic Endpoint security	https://cybersecuritynews.com/paloalto-to-acquire-koi-security/
New Malware Campaign 'CRESCENTHARVEST' Exploits Iran Protest Sentiment to Deploy Information-Stealing RAT	https://cybersecuritynews.com/new-malware-campaign-crescentharvest-exploits-iran-protest/

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
AI Dev Tool Cline's npm Token Hijacked by Hackers for 8 Hours	https://cybersecuritynews.com/ai-dev-tool-cline/
Those 'Summarize With AI' Buttons May Be Lying to You	https://www.darkreading.com/application-security/supply-chain-attack-openclaw-cline-users
Adidas Investigates Alleged Data Breach – 815,000 Records of Customer Data Stolen	https://cybersecuritynews.com/adidas-investigates-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
Grandstream GXP1600 VoIP Phones Exposed to Unauthenticated Remote Code Execution	https://thehackernews.com/2026/02/grandstream-gxp1600-voip-phones-exposed.html
Critical Flaws Found in Four VS Code Extensions with Over 125 Million Installs	https://thehackernews.com/2026/02/critical-flaws-found-in-four-vs-code.html
Dell RecoverPoint for VMs Zero-Day CVE-2026-22769 Exploited Since Mid-2024	https://thehackernews.com/2026/02/dell-recoverpoint-for-vms-zero-day-cve.html
CISA Flags Four Security Flaws Under Active Exploitation in Latest KEV Update	https://thehackernews.com/2026/02/cisa-flags-four-security-flaws-under.html
Vulnerabilities in Popular PDF Platforms Allowed Account Takeover, Data Exfiltration	https://www.securityweek.com/vulnerabilities-in-popular-pdf-platforms-allowed-account-takeover-data-exfiltration/
CISA: Hackers Exploiting Vulnerability in Product of Taiwan Security Firm TeamT5	https://www.securityweek.com/cisa-hackers-exploiting-vulnerability-in-product-of-taiwan-security-firm-teamt5/
Dell RecoverPoint Zero-Day Exploited by Chinese Cyberespionage Group	https://www.securityweek.com/dell-recoverpoint-zero-day-exploited-by-chinese-cyberespionage-group/
Critical Grandstream VoIP Bug Highlights SMB Security Blind Spot	https://www.darkreading.com/threat-intelligence/grandstream-bug-voip-security-blind-spot
Telegram channels expose rapid weaponization of SmarterMail flaws	https://www.bleepingcomputer.com/news/security/telegram-channels-expose-rapid-weaponization-of-smartermail-flaws/
Critical infra Honeywell CCTVs vulnerable to auth bypass flaw	https://www.bleepingcomputer.com/news/security/critical-infra-honeywell-cctvs-vulnerable-to-auth-bypass-flaw/
Flaws in Popular Software Development App Extensions Allow Data Exfiltration	https://www.infosecurity-magazine.com/news/vulnerabilities-vs-code-cursor/
Researchers Reveal Six New OpenClaw Vulnerabilities	https://www.infosecurity-magazine.com/news/researchers-six-new-openclaw/
Microsoft 365 Copilot Flaw Allows AI Assistant to Summarize Sensitive Emails	https://cybersecuritynews.com/microsoft-365-copilot-bug/
Critical Ivanti EPMM Zero-Day Vulnerabilities Exploited in The Wild Targeting Corporate Networks	https://cybersecuritynews.com/critical-ivanti-epmm-zero-day-vulnerabilities/
Single-Character Typo of “&” Instead of “|” Leads to 0-Day RCE in Firefox	https://cybersecuritynews.com/firefox-0-day-rce/
CISA Warns of Google Chromium 0-Day Vulnerability Actively Exploited in Attacks	https://cybersecuritynews.com/google-chromium-0-day-vulnerability/
Beyond CVE China’s Dual Vulnerability Databases Reveal a Different Disclosure Timeline	https://cybersecuritynews.com/beyond-cve-chinas-dual-vulnerability-databases/

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
Notepad++ Fixes Hijacked Update Mechanism Used to Deliver Targeted Malware	https://thehackernews.com/2026/02/notepad-fixes-hijacked-update-mechanism.html
Anthropic Releases Claude Sonnet 4.6 with Improved Coding, Computer Use, and 1M Token Context Window	https://cybersecuritynews.com/claude-sonnet-4-6-released/
OpenAI Launches EVMbench to Detect, Patch, and Exploit Vulnerabilities in Blockchain Environments	https://cybersecuritynews.com/openai-evmbench/
OpenClaw AI Framework v2026.2.17 Released with Anthropic Model Support and Security Fixes	https://cybersecuritynews.com/openclaw-ai-framework-v2026-2-17/
Microsoft Patches CVE-2026-26119 Privilege Escalation in Windows Admin Center	https://thehackernews.com/2026/02/microsoft-patches-cve-2026-26119.html

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
Cryptojacking Campaign Exploits Driver to Boost Monero Mining	https://www.infosecurity-magazine.com/news/cryptojacking-driver-boost-monero/
AI Assistants Used as Covert Command-and-Control Relays	**https://www.infosecurity-magazine.com/news/ai-assistants-covert-c2-relays/**
Malware Campaign Delivers Remote Access Backdoor and Fake MetaMask Wallet to Steal Cryptocurrency Funds	https://cybersecuritynews.com/malware-campaign-delivers-remote-access-backdoor-and-fake-metamask-wallet/
Credit Card Fraud Emerges with a New Sophisticated Carding-as-a-Service Marketplaces	https://cybersecuritynews.com/credit-card-fraud-emerges/
Hackers Leveraging Emoji Code to Hide Malicious Code and Evade Security Detections	https://cybersecuritynews.com/hackers-leveraging-emoji-code/
MCP Servers can be Exploited to Execute Arbitrary Code and Exfiltrate Sensitive Data	https://cybersecuritynews.com/mcp-servers-can-be-exploited/
Fake CAPTCHA (ClickFix) Attack Chain Leads to Enterprise-Wide Malware Infection in Organisations	https://cybersecuritynews.com/fake-captcha-clickfix-attack-chain/
ClickFix Abuses Legitimate Homebrew Workflow to Deploy Cuckoo Stealer on macOS for Credential Harvesting	https://cybersecuritynews.com/clickfix-abuses-legitimate-homebrew-workflow/
ClawHavoc Poisoned OpenClaw's ClawHub with 1,184 Malicious Skills, Enabling Data Theft and Backdoor Access	https://cybersecuritynews.com/clawhavoc-poisoned-openclaws-clawhub/
New Phishing Campaign Targets Booking.com Partners and Customers in Multi-Stage Financial Fraud Scheme	https://cybersecuritynews.com/new-phishing-campaign-targets-booking-com-partners-and-customers/

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 Tools for Enterprise Security Monitoring	**https://cybersecuritynews.com/enterprise-security-monitoring-tools/**
Splunk Releases Guide to Detect Remote Employment Fraud Within Your Organization	https://cybersecuritynews.com/detect-remote-employment-fraud/
ThreatBook Launches Best-of-Breed Advanced Threat Intelligence Solution	https://cybersecuritynews.com/threatbook-advanced-threat-intelligence-solution/
CISA Releases Best Security Practices Guide for Hardening Microsoft Exchange Server	https://cybersecuritynews.com/microsoft-exchange-server-hardening-guide/
Top 10 Best Exposure Management Tools In 2026	https://cybersecuritynews.com/best-exposure-management-tools/
NETREAPER Offensive Security Toolkit That Wraps 70+ Penetration Testing Tools	https://cybersecuritynews.com/netreaper-offensive-security-toolkit/
GitLab Security Best Practices Cheat Sheet	https://thehackernews.uk/gitlab-security-tips
False Negatives Are a New SOC Headache. Here's the Fast Way to Fix It	https://cybersecuritynews.com/false-negatives-are-a-new-soc-headache-heres-the-fast-way-to-fix-it/
PentAGI – Automated AI-Powered Penetration Testing Tool that Integrates 20+ Security Tools	https://cybersecuritynews.com/pentagi-penetration-testing-tool/

References

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

[2]. Τα CVEs αποτελέσματα που εμφανίζονται στην ενότητα 1 διαθέτουν 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/