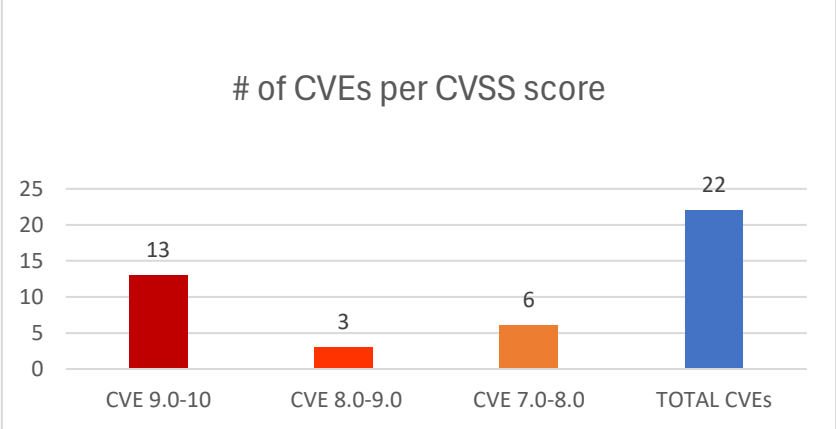
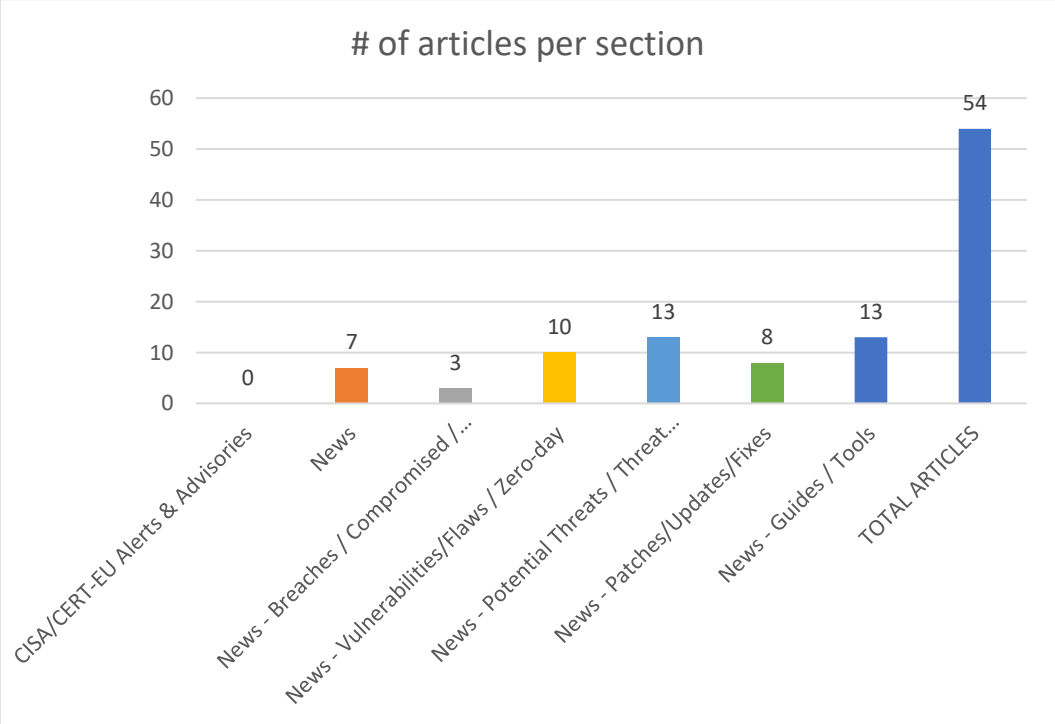
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 08/07/2026 - 10/07/2026





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-2026-54769	10,0	Langroid	Improper Control of Generation of Code ('Code Injection')	prior to 0.65.2	https://github.com/langroid/langroid/security/advisories/GHSA-q9p7-wqxg-mrhc
https://nvd.nist.gov/vuln/detail/CVE-2026-58123	9,8	Hermes WebUI	Missing Authentication for Critical Function	before 0.51.788	https://github.com/nesquena/hermes-webui/commit/d257e5f36cfa9328600c8bde6f0de09a6ad9b6f4 VulnCheck https://github.com/nesquena/hermes-webui/pull/5268 VulnCheck https://github.com/nesquena/hermes-webui/releases/tag/v0.51.788 VulnCheck https://www.vulncheck.com/advisories/hermes-webui-unauthenticated-rce-via-terminal-api
https://nvd.nist.gov/vuln/detail/CVE-2026-15282	9,8	The Instant Appointment plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 1.2	https://plugins.trac.wordpress.org/browser/instant-appointment/trunk/includes/ajax/ajax_services.php#L3 Wordfence https://plugins.trac.wordpress.org/browser/instant-appointment/trunk/includes/front-end/ajax/login_ajax.php#L584 Wordfence https://plugins.trac.wordpress.org/browser/instant-appointment/trunk/includes/front-end/ajax/login_ajax.php#L598 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/097b1530-64fa-45b2-85f3-c6a2311405b5?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2026-8801	9,8	Progress MOVEit Transfer	Path Equivalence: 'filename ' (Trailing Space)	before 2025.0.8, from 2025.1.0 before 2025.1.4	https://docs.progress.com/bundle/moveit-transfer-release-notes-2026/page/Fixed-Issues-in-2026.html
https://nvd.nist.gov/vuln/detail/CVE-2026-9695	9,8	DELMIA Apriso	Improper Authentication	from Release 2020 through Release 2026	https://www.3ds.com/trust-center/security/security-advisories/cve-2026-9695
https://nvd.nist.gov/vuln/detail/CVE-2026-14894	9,8	The Super Forms – Drag & Drop Form Builder plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 6.3.313	https://github.com/RensTillmann/super-forms/commit/c5838f5877c72b738c54ed970935c77ae6830c3a Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/e9c7fb16-efbb-41e9-be13-98e96c1e9100?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-44024	9,8	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Prior to 1.19.3	https://github.com/fluent/fluentd/commit/45c87a81f3ac0b72b3f9dcfe8cfb5f9038f81437 GitHub, Inc. https://github.com/fluent/fluentd/pull/5391 GitHub, Inc. https://github.com/fluent/fluentd/releases/tag/v1.19.3 GitHub, Inc. https://github.com/fluent/fluentd/security/advisories/GHSA-44hj-4m45-frj3
https://nvd.nist.gov/vuln/detail/CVE-2026-15113	9,6	Autofill in Google Chrome on Android	Use After Free	prior to 150.0.7871.115	https://chromereleases.googleblog.com/2026/07/stable-channel-update-for-desktop_01162222768.html Chrome Release Notes Vendor Advisory https://issues.chromium.org/issues/520540744
https://nvd.nist.gov/vuln/detail/CVE-2026-15062	9,6	Snowflake Snowpark Python SDK	Improper Neutralization of Special Elements used	prior to 1.53.0	https://github.com/snowflakedb/snowpark-python/blob/main/CHANGELOG.md

			in an SQL Command ('SQL Injection')		
https://nvd.nist.gov/vuln/detail/CVE-2026-59702	9,3	repomix	Server-Side Request Forgery (SSRF)		https://github.com/CrazyForks/repomix/commit/c748b524f41225e7fc6f89ad0084520901a453cf VulnCheck https://github.com/yamadashy/repomix VulnCheck https://github.com/yamadashy/repomix/issues/1703 CISA-ADP, VulnCheck https://www.vulncheck.com/advisories/repomix-server-side-request-forgery-via-unvalidated-repository-urls-in-post-api-pack
https://nvd.nist.gov/vuln/detail/CVE-2026-59826	9,1	Metabase	Improper Control of Generation of Code ('Code Injection')	From 1.55.0 until 1.58.15.1, 1.59.12, 1.60.6.3, and 1.61.2	https://github.com/metabase/metabase/commit/74032e5e0a5a70dc45a6a744d37b9ba24eee8d01 GitHub, Inc. https://github.com/metabase/metabase/releases/tag/v0.58.15.1 GitHub, Inc. https://github.com/metabase/metabase/releases/tag/v0.59.12 GitHub, Inc. https://github.com/metabase/metabase/releases/tag/v0.60.6.3 GitHub, Inc. https://github.com/metabase/metabase/releases/tag/v0.61.2 GitHub, Inc. https://github.com/metabase/metabase/security/advisories/GHSA-8wx2-rxp2-4x35
https://nvd.nist.gov/vuln/detail/CVE-2026-9074	9,1	IBM API Connect	Improper Neutralization of Special Elements	10.0.8.0 through 10.0.8.9 and 12.1.0.0 through 12.1.0.3	https://www.ibm.com/support/pages/node/7278218 IBM Corporation https://www.ibm.com/support/pages/node/7278909

			used in an SQL Command ('SQL Injection')		
https://nvd.nist.gov/vuln/detail/CVE-2026-15300	9,1	The GEO my WP plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to, and including, 4.5.4	https://plugins.trac.wordpress.org/browser/geo-my-wp/tags/4.5.4/plugins/posts-locator/includes/class-gmw-wp-query.php#L299 Wordfence https://plugins.trac.wordpress.org/browser/geo-my-wp/tags/4.5.4/plugins/posts-locator/includes/class-gmw-wp-query.php#L300 Wordfence https://plugins.trac.wordpress.org/browser/geo-my-wp/tags/4.5.4/plugins/posts-locator/includes/class-gmw-wp-query.php#L301 Wordfence https://plugins.trac.wordpress.org/browser/geo-my-wp/tags/4.5.5/plugins/posts-locator/includes/class-gmw-wp-query.php#L286 Wordfence https://plugins.trac.wordpress.org/browser/geo-my-wp/tags/4.5.5/plugins/posts-locator/includes/class-gmw-wp-query.php#L305 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/ecbc7f05-fc4f-4276-968e-04222a64e55a?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-60102	8,8	Horde Virtual File System (VFS) API	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	before 3.0.1	https://github.com/horde/Vfs/commit/41f74b4acfc144e09013d04dd121e0a5da808361 VulnCheck https://github.com/horde/Vfs/pull/10 VulnCheck https://github.com/horde/Vfs/releases/tag/v3.0.1 VulnCheck https://www.vulncheck.com/advisories/horde-vfs-os-command-injection-via-horde-vfs-smb-driver

https://nvd.nist.gov/vuln/detail/CVE-2026-60104	8,7	Bitwarden Server	Authorization Bypass Through User-Controlled Key	before 2026.6.0	https://github.com/bitwarden/server/commit/dcf4c486b2b5bedecc03a48b427243328cc74a9a VulnCheck https://github.com/bitwarden/server/pull/7615 VulnCheck https://github.com/bitwarden/server/releases#release-v2026.6.0 VulnCheck https://sanjokkarki.com.np/blog/bitwarden-vault-key-heist VulnCheck https://www.vulncheck.com/advisories/bitwarden-server-authorization-bypass-via-admin-auth-request
https://nvd.nist.gov/vuln/detail/CVE-2026-60105	8,6	Monsta FTP	Server-Side Request Forgery (SSRF)	before 2.14.5	https://www.monstaftp.com/notes/ VulnCheck https://www.vulncheck.com/advisories/monsta-ftp-ssrf-via-ipv4-mapped-ipv6-address-bypass
https://nvd.nist.gov/vuln/detail/CVE-2026-60109	7,5	Zeek	NULL Pointer Dereference	before 8.0.9	https://github.com/zeek/zeek/commit/c82e3c734893d932e94310aec0dbeb1ffcea169d VulnCheck https://github.com/zeek/zeek/releases/tag/v8.0.9 VulnCheck https://www.vulncheck.com/advisories/zeek-null-pointer-dereference-dos-via-kerberos-krb-error-parsing
https://nvd.nist.gov/vuln/detail/CVE-2026-59925	7,5	Mistune	Inefficient Regular Expression Complexity	Prior to 3.3.0	https://github.com/lepture/mistune/commit/5de41fb8e527004dbc363e047a3c380c9288c74f GitHub, Inc. Patch https://github.com/lepture/mistune/releases/tag/v3.3.0 GitHub, Inc. Release Notes https://github.com/lepture/mistune/security/advisories/GHSA-4j32-57v6-6g45
https://nvd.nist.gov/vuln/detail/CVE-2026-59937	7,5	pypdf	Uncontrolled Resource	Prior to 6.14.0	https://github.com/py-pdf/pypdf/commit/b5fc5aa714f4b696fb9b1deaa35a9e4a4eb50dae GitHub, Inc. Patch https://github.com/py-pdf/pypdf/pull/3887 GitHub, Inc.

			Consumption		Issue Tracking Patch https://github.com/py-pdf/pypdf/releases/tag/6.14.0 GitHub, Inc. Product Release Notes https://github.com/py-pdf/pypdf/security/advisories/GHSA-55h5-xmcq-c37v
https://nvd.nist.gov/vuln/detail/CVE-2026-59939	7,5	httplib2	Improper Handling of Highly Compressed Data (Data Amplification)	Prior to 0.32.0	https://github.com/httplib2/httplib2/commit/87581ad6cf752fe3da2090c59058261d2d00a427 GitHub, Inc. https://github.com/httplib2/httplib2/releases/tag/v0.32.0 GitHub, Inc. https://github.com/httplib2/httplib2/security/advisories/GHSA-j5g9-f88f-gfj3
https://nvd.nist.gov/vuln/detail/CVE-2026-61343	7,2	LibreBooking's email	Relative Path Traversal		https://github.com/LibreBooking/librebooking/commit/cb9b7ad9da0243bd105809f6a4a8a6b9147c71ea
https://nvd.nist.gov/vuln/detail/CVE-2026-59948	7,0	Composer	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Prior to 2.2.29 and 2.10.2	https://github.com/composer/composer/commit/502c6c4f699802d9cf464728b3e8a95674f919a0

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
-	-	-

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
OpenAI Releases GPT-5.6 and ChatGPT Work, a New Companion to Handle Your Tasks	https://cybersecuritynews.com/openai-gpt-5-6-and-chatgpt-work/
Microsoft Adopts AI-Powered Scanning to Find Vulnerabilities Before Attackers	https://cybersecuritynews.com/microsoft-adopts-ai-vulnerability-scanning/
Anthropic Extends Free Access to Claude Fable 5 on All Paid Plans	https://cybersecuritynews.com/anthropic-extends-fable-5-access/
OpenAI Reportedly Secures US Government Clearance to Launch GPT-5.6 Model	https://cybersecuritynews.com/openai-gpt-5-6-model/
CISA orders feds to prioritize patching Langflow auth bypass flaw	https://www.bleepingcomputer.com/news/security/cisa-orders-feds-to-prioritize-patching-langflow-auth-bypass-flaw/
75% CISOs Fear Executives Don’t Understand Cybersecurity Risks Employees Face	https://www.infosecurity-magazine.com/news/cisos-fear-execs-dont-understand/
Chinese-Funded Interpol Cybercrime Crackdown Leads to 5,800 Arrests	https://www.infosecurity-magazine.com/news/china-interpol-cybercrime-crackdown/

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
A Hacker Used AI to Compromise an AWS Cloud Environment in Just 72 Hours	https://cybersecuritynews.com/aws-cloud-compromise-in-72-hours/
AssuranceAmerica Data Breach Exposed 6.9 Million People's License Numbers and Personal Data	https://cybersecuritynews.com/assuranceamerica-data-breach/
Discord's Security Systems Mistakenly Banned 8,000+ Accounts Since May 2026	https://cybersecuritynews.com/discords-systems-users-banned/

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
RoundCube 0-Click Vulnerability Enables Stored XSS Attack via MIME Type Attachment	https://cybersecuritynews.com/roundcube-0-click-vulnerability/
HP Linux Printing Software Vulnerability Allows Remote Attackers to Execute Arbitrary Code	https://cybersecuritynews.com/hp-linux-printing-software-vulnerability/
Linux Kernel Vulnerability Enables Passwordless Root Through DRM Render Nodes	https://cybersecuritynews.com/linux-kernel-bug-passwordless-root/
15-year-old GhostLock Kernel Flaw Enables Privilege Escalation in Major Linux Distributions	https://cybersecuritynews.com/15-year-old-ghostlock-linux-kernel-vulnerability/
70% of WordPress Sites Running Outdated PHP Versions Exposed to Cyberattacks	https://cybersecuritynews.com/wordpress-sites-running-outdated-php-versions-exposed/
CISA Warns of Adobe ColdFusion Path Traversal Vulnerability Exploited in Attacks	https://cybersecuritynews.com/adobe-coldfusion-path-traversal-exploited/
First-Ever 1- Click Android 17 Exploit Allows Attackers to Gain Full Control Over Your Android Phone	https://cybersecuritynews.com/android-17-root-1-click/
New GhostApproval Vulnerability Affects Amazon Q, Claude Code, Cursor, and Other AI Agents	https://cybersecuritynews.com/ghostapproval-vulnerability/
GitHub Copilot Refuses Harmful Chat Prompts But Writes Them Inside Code Workflows	https://cybersecuritynews.com/github-copilot-refuses-harmful-chat-prompts/
CISA Adds 4 Actively Exploited Adobe, Joomla, and Langflow Flaws to KEV	https://thehackernews.com/2026/07/cisa-adds-4-actively-exploited-adobe.html

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
Wireshark 4.6.7 Released With Fixes for Vulnerabilities Allowing Crashes via Malicious Packets	https://cybersecuritynews.com/wireshark-4-6-7-released/
20 Remote Code Execution Vulnerabilities Patched in Foxit PDF Reader and Editor	https://cybersecuritynews.com/foxit-pdf-reader-and-editor-vulnerabilities/
GitLab Patches Eight Security Vulnerabilities Across Community and Enterprise Editions	https://cybersecuritynews.com/gitlab-patches-security-vulnerabilities/
Microsoft Releases Patch for RoguePlanet Defender Zero-Day Vulnerability	https://cybersecuritynews.com/rogueplanet-defender-zero-day-vulnerability/
Accenture Data Breach – Hackers Allegedly Claim to Have Stolen 35 GB of Source Code	https://cybersecuritynews.com/accenture-data-breach/
Chrome Update Patches 27 Vulnerabilities including Two Code Execution Flaws	https://cybersecuritynews.com/chrome-update-patches-27-vulnerabilities/
Ubiquiti Patches Critical UniFi Flaws Across Connect, Talk, Access, Protect, and OS	https://thehackernews.com/2026/07/ubiquiti-patches-critical-unifi-flaws.html
Palo Alto Networks Patches 13 Vulnerabilities	https://www.securityweek.com/palo-alto-networks-patches-13-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
GodDamn Ransomware Rebrands From Beast and Uses PoisonX Driver to Disable Defenses	https://cybersecuritynews.com/goddamn-ransomware-rebrands-from-beast/
ACSC Warns of Large-Scale CMS Exploitation Campaign Deploys Webshells on Vulnerable Websites	https://cybersecuritynews.com/acsc-warns-of-large-scale-cms-exploitation-campaign-deploys-webshells/
Hackers Abuse Microsoft Entra Passkey Enrollment to Hijack Enterprise Accounts	https://cybersecuritynews.com/hackers-abuse-microsoft-entra-passkey-enrollment/
Windows Update Silently Installs LG Monitor App That Pushes McAfee Ads	https://cybersecuritynews.com/windows-update-installs-lg-monitor-app-pushes-mcafee-ads/
UNC6692 Hackers Uses Microsoft Teams Helpdesk Impersonation to Deploy SNOW Malware	https://cybersecuritynews.com/unc6692-hackers-uses-microsoft-teams-helpdesk-impersonation/
AI Double Agent Attack Turns Claude Desktop to Execute Remote Code on a Target Machine	https://cybersecuritynews.com/mycelium-framework-first-ever-know-botnet/
CrowdStrike Unveils 5 New Prompt Injection Techniques Challenging AI Agents	https://cybersecuritynews.com/5-new-prompt-injection-techniques/
Fake Indian ITR Notice Delivers Dual RAT Malware Through Six-Stage Infection Chain	https://cybersecuritynews.com/fake-indian-itr-notice-delivers-dual-rat-malware/
Lurking Lizard Uses Fake 7-Zip Installers to Turn Victim Devices Into Proxy Nodes	https://cybersecuritynews.com/lurking-lizard-uses-fake-7-zip-installers/

APT-C-20 Hackers Hide Shellcode in PNG Images to Launch Fileless C# Backdoor	https://cybersecuritynews.com/apt-c-20-hackers-hide-shellcode-in-png-images/
New HalluSquatting Attack Could Trick AI Coding Assistants Into Installing Botnet Malware	https://thehackernews.com/2026/07/new-hallusquatting-attack-could-trick.html
Unpatched Backdoor in Tenda Firmware Grants Admin Access to Devices	https://www.securityweek.com/unpatched-backdoor-in-tenda-firmware-grants-admin-access-to-devices/
China-Linked APT Expands Proxy Network With New Malware	https://www.infosecurity-magazine.com/news/uat-7810-china-apt-orb-proxy/

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/
The CISO Executive Toolkit (Free Download)	https://thehackernews.uk/wiz-ciso-bundle
Secure Coding Best Practices: Practical Guide + Cheat Sheet for Developers	https://thehackernews.uk/secure-coding-wiz-cheat
Top 10 Best Malware Sandbox Tools for Security Teams in 2026	https://cybersecuritynews.com/best-malware-sandbox-tools/
Top 5 Best Tools for Simulated DDoS Attacks in 2026	https://cybersecuritynews.com/simulated-ddos-attacks/

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/