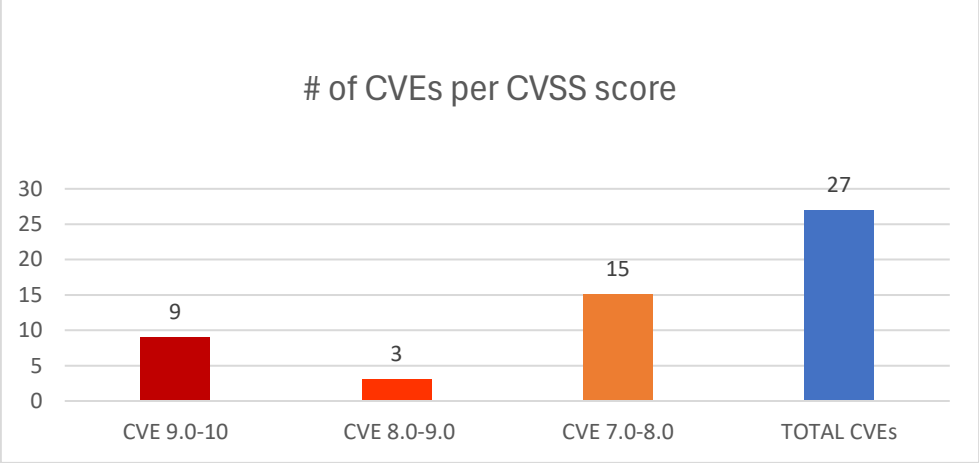
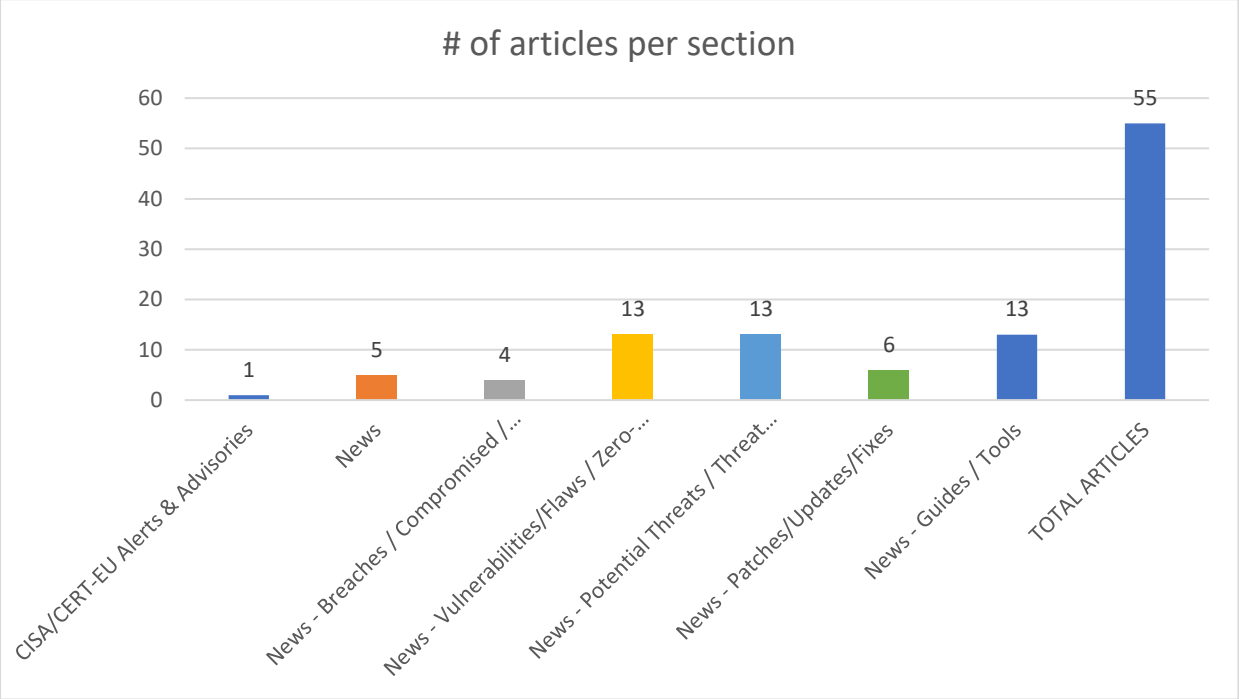
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 06/06/2026 - 09/06/2026





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-2023-54352	9,8	WordPress Seotheme	Missing Authentication for Critical Function		https://www.exploit-db.com/exploits/51789 VulnCheck https://www.vulncheck.com/advisories/wordpress-seotheme-remote-code-execution-unauthenticated
https://nvd.nist.gov/vuln/detail/CVE-2024-58348	9,8	WordPress Background Image Cropper	Unrestricted Upload of File with Dangerous Type	1.2	https://wordpress.org VulnCheck https://wordpress.org/plugins/background-image-cropper/ VulnCheck https://www.exploit-db.com/exploits/51998 VulnCheck https://www.vulncheck.com/advisories/wordpress-background-image-cropper-remote-code-execution
https://nvd.nist.gov/vuln/detail/CVE-2024-58349	9,8	WordPress Theme Travelscape	Unrestricted Upload of File with Dangerous Type	1.0.3	https://www.exploit-db.com/exploits/51969 VulnCheck https://www.vulncheck.com/advisories/wordpress-theme-travelscape-arbitrary-file-upload
https://nvd.nist.gov/vuln/detail/CVE-2026-52778	9,8	YesWiki	Improper Control of Generation of Code ('Code Injection')	Prior to version 4.6.6	https://github.com/YesWiki/yeswiki/commit/dd2bd8fb099de0d21504bda8a810693b3fcb8e52 GitHub, Inc. https://github.com/YesWiki/yeswiki/releases/tag/v4.6.6 GitHub, Inc. https://github.com/YesWiki/yeswiki/security/advisories/GHSA-px5m-h76g-p7p8
https://nvd.nist.gov/vuln/detail/CVE-2026-25555	9,8	OpenBullet2	Authentication Bypass by Primary Weakness	through version 0.3.2	https://hackernoon.com/one-empty-header-to-admin-how-an-auth-bypass-breaks-openbullet2 VulnCheck

					https://www.vulncheck.com/advisories/openbullet2-authentication-bypass-via-x-api-key-header
https://nvd.nist.gov/vuln/detail/CVE-2026-5067	9,8	Zephyr's HTTP server WebSocket	Out-of-bounds Write		https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-wgr4-9pwq-94vj
https://nvd.nist.gov/vuln/detail/CVE-2026-39910	9,8	STACKIT IaaS API	Missing Authorization		https://status.stackit.cloud VulnCheck https://www.vulncheck.com/advisories/stackit-iaas-api-privilege-escalation-via-service-account-attachment
https://nvd.nist.gov/vuln/detail/CVE-2026-41448	9,4	AdGuard Home	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')		https://github.com/AdguardTeam/AdGuardHome/releases/tag/v0.107.77 VulnCheck https://www.vulncheck.com/advisories/adguard-home-authentication-bypass-via-path-traversal-in-admin-token-cookie
https://nvd.nist.gov/vuln/detail/CVE-2026-11393	9,0	AgentCore CLI	Improper Control of Generation of Code ('Code Injection')	before v0.14.2	https://aws.amazon.com/security/security-bulletins/2026-040-aws/ AMZN https://github.com/aws/agentcore-cli/releases/tag/v0.14.2 AMZN https://github.com/aws/agentcore-cli/security/advisories/GHSA-m4x6-gwgp-4pm7 AMZN https://www.npmjs.com/package/@aws/agentcore/v/0.14.2 AMZN https://www.npmjs.com/package/@aws/agentcore/v/1.0.0-preview.9
https://nvd.nist.gov/vuln/detail/CVE-2026-11413	8,8	JingDong JD Cloud Box AX6600	Stack-based Buffer Overflow	4.5.3.r4546	http://cdn2.v50to.cc/JDcloud-AX6600_overflow.zip VulDB https://vuldb.com/cve/CVE-2026-11413 VulDB https://vuldb.com/submit/820025 VulDB https://vuldb.com/vuln/368970 VulDB https://vuldb.com/vuln/368970/cti

https://nvd.nist.gov/vuln/detail/CVE-2026-26422	8,4	clash-verge-service-ipc	Incorrect Permission Assignment for Critical Resource	before 2.3.0	https://github.com/clash-verge-rev/clash-verge-rev/commit/3bbcdbe5caacc2ffb713af69f2c93e202573f918 MITRE https://github.com/clash-verge-rev/clash-verge-service-ipc/releases/tag/v2.3.0 MITRE https://kaguranaku.me/posts/CVE-2026-26422/
https://nvd.nist.gov/vuln/detail/CVE-2026-9662	8,1	The Recover Exit For WooCommerce plugin for WordPress	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion	up to and including 1.0.3	https://plugins.trac.wordpress.org/browser/recoverexit-for-woocommerce/tags/1.0.3/recover_exit_main.php#L41
https://nvd.nist.gov/vuln/detail/CVE-2026-49494	7,5	Comodo Internet Security's firewall driver Inspect.sys	Integer Underflow (Wrap or Wraparound)		https://github.com/MalwareTech/ComoDoS VulnCheck https://malwaretech.com/2026/06/exploiting-a-remote-kernel-vulnerability-in-comodo-internet-security.html VulnCheck https://www.vulncheck.com/advisories/comodo-internet-security-inspect-sys-ipv6-integer-underflow-remote-denial-of-service
https://nvd.nist.gov/vuln/detail/CVE-2026-41842	7,5	Spring MVC and WebFlux	Uncontrolled Resource Consumption	Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48	https://spring.io/security/cve-2026-41842
https://nvd.nist.gov/vuln/detail/CVE-2026-41720	7,4	Spring LDAP's DirContextAuthenticationStrategy	Improper Authentication	Spring LDAP 2.4.0 through 2.4.4; 3.2.0 through 3.2.17; 3.3.0 through 3.3.7; 4.0.0 through 4.0.3	https://spring.io/security/cve-2026-41720
https://nvd.nist.gov/vuln/detail/CVE-2026-11435	7,3	Jinher OA	Improper Neutralization of Special Elements used in an	1.0	https://github.com/Mr-Elymas/cve_submit/issues/1 VulDB https://vuldb.com/cve/CVE-2026-11435 VulDB https://vuldb.com/submit/822114 VulDB

			SQL Command ('SQL Injection')		https://vuldb.com/vuln/369015 VulDB https://vuldb.com/vuln/369015/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-11437	7,3	go-fastdfs-web	Server-Side Request Forgery (SSRF)	up to 1.3.7	https://vuldb.com/cve/CVE-2026-11437 VulDB https://vuldb.com/submit/822726 VulDB https://vuldb.com/vuln/369017 VulDB https://vuldb.com/vuln/369017/cti VulDB https://www.notion.so/Server-Side-Request-Forgery-SSRF-in-go-fastdfs-web-Installation-Endpoint-35aea92a3c41806485ffeeac7e18126a
https://nvd.nist.gov/vuln/detail/CVE-2026-11451	7,3	GL.iNet GL-MT3000	Improper Neutralization of Special Elements used in a Command ('Command Injection')	4.4.5	https://github.com/StrTzz123/iot_vul/blob/main/GL-iNet/MT3000/4.4.5/nas_proto_media_dir_glc_rce/Readme.md VulDB https://vuldb.com/cve/CVE-2026-11451 VulDB https://vuldb.com/submit/825563 VulDB https://vuldb.com/vuln/369071 VulDB https://vuldb.com/vuln/369071/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-11462	7,3	Chengdu Everbrite Network Technology BeikeShop	Improper Authorization	up to 1.6.0.22	https://github.com/beikeshop/beikeshop/commit/6719e0fc690ea0a998452092862e0f0a17c65968 VulDB https://github.com/nuiifornet/BeikeShop-Vulnerability/blob/main/README.md VulDB https://vuldb.com/cve/CVE-2026-11462 VulDB https://vuldb.com/submit/831466 VulDB https://vuldb.com/vuln/369082 VulDB https://vuldb.com/vuln/369082/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-11463	7,3	USCiLab Cereal	Access of Resource Using Incompatible Type ('Type Confusion')	up to 1.3.2	https://gist.github.com/TrebledJ/0223c1fa3c3fd64e2c7047b8a4385ec0 VulDB https://github.com/USCiLab/cereal/ VulDB https://github.com/USCiLab/cereal/issues/870 VulDB https://vuldb.com/cve/CVE-2026-11463 VulDB https://vuldb.com/submit/814456 VulDB

					https://vuldb.com/vuln/369083 VulDB https://vuldb.com/vuln/369083/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-11471	7,3	SourceCodester Class and Exam Timetabling System	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	1.0	https://github.com/Icecream102/cve/issues/4 VulDB https://vuldb.com/cve/CVE-2026-11471 VulDB https://vuldb.com/submit/833858 VulDB https://vuldb.com/vuln/369091 VulDB https://vuldb.com/vuln/369091/cti VulDB https://www.sourcecodester.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-11474	7,3	Kushan2k student-management-system	Improper Access Control	up to f16a4ceaddd6729c4b306ed4641cda3176c1ef2a	https://github.com/Kushan2k/student-management-system/ VulDB https://github.com/Kushan2k/student-management-system/issues/1 VulDB https://vuldb.com/cve/CVE-2026-11474 VulDB https://vuldb.com/submit/833933 VulDB https://vuldb.com/vuln/369094 VulDB https://vuldb.com/vuln/369094/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-11488	7,3	Simple Flight Ticket Booking System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ VulDB https://github.com/K1venn/cves/issues/1 VulDB https://vuldb.com/cve/CVE-2026-11488 VulDB https://vuldb.com/submit/834511 VulDB https://vuldb.com/vuln/369108 VulDB https://vuldb.com/vuln/369108/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-11489	7,3	Online Music Site	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ VulDB https://github.com/11snk/CVE/issues/2 VulDB https://vuldb.com/cve/CVE-2026-11489 VulDB https://vuldb.com/submit/834743 VulDB https://vuldb.com/vuln/369109 VulDB https://vuldb.com/vuln/369109/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-11457	7,3	erzhongxmu JeeWMS	Improper Neutralization	up to 141740afb2ba14d441c82a833d0a418d07ca2d69	https://github.com/0d000721999/evc1/issues/1 VulDB https://vuldb.com/cve/CVE-2026-11457 VulDB https://vuldb.com/submit/828509 VulDB

					https://vuldb.com/vuln/369076 VulDB https://vuldb.com/vuln/369076/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-9851	7,2	The Booking Package plugin for WordPress			https://plugins.trac.wordpress.org/browser/booking-package/tags/1.7.13/index.php#L4416 Wordfence https://plugins.trac.wordpress.org/browser/booking-package/tags/1.7.13/index.php#L4477 Wordfence https://plugins.trac.wordpress.org/browser/booking-package/tags/1.7.13/lib/Schedule.php#L868 Wordfence https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3558752%40booking-package&new=3558752%40booking-package&sfp_email=&sfph_mail= Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/795c1fd6-137b-4414-8d6b-30053bfb5924?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-7537	7,2	he MDJM Event Management plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 1.7.8.3	https://github.com/d0n601/CVE-2026-7537

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-2026-42271 BerriAI LiteLLM Command Injection Vulnerability** ▪ **CVE-2026-50751 Check Point Security Gateway Improper Authentication Vulnerability**	**https://www.cisa.gov/news-events/alerts/2026/06/08/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
Emphere Raises $2.1 Million for AI-Powered Vulnerability Remediation	https://www.securityweek.com/emphere-raises-2-1-million-for-ai-powered-vulnerability-remediation/
OWASP Incubator Project Helps Developers Find and Fix Vulnerable Dependencies in Seconds	https://www.securityweek.com/owasp-incubator-project-helps-developers-find-and-fix-vulnerable-dependencies-in-seconds/
Exposed Fuel Tank Gauges Under Attack in the US	https://www.darkreading.com/cyberattacks-data-breaches/exposed-fuel-tank-gauges-attack-us
OWASP CVE Lite CLI – New Tool to Scan for Vulnerabilities in Your Projects	https://cybersecuritynews.com/owasp-cve-lite-cli-tool/
Two-Thirds of Open Source Community Unaware of Cyber Resilience Act	https://www.infosecurity-magazine.com/news/open-source-unaware-cyber/

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
Hola Browser for Windows Delivery Pipeline Compromised to Deliver Cryptominer	https://cybersecuritynews.com/hola-browser-for-windows-delivery-pipeline-compromised/
New Shai-Hulud Attack Compromises 23 PyPI Packages to Target MCP Developers	https://cybersecuritynews.com/23-pypi-packages-compromised/
Meta AI Bug Exposes Over 20,000 Instagram Accounts	https://www.infosecurity-magazine.com/news/over-20000-instagram-accounts/
Internet Explorer WebBrowser Control Attack Chain Turns Clicks Into RCE	https://cybersecuritynews.com/internet-explorer-webbrowser-attack/

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
Cisco Catalyst SD-WAN Manager CVE-2026-20245 Flaw Actively Exploited – No Patch Available	https://thehackernews.com/2026/06/cisco-catalyst-sd-wan-manager-cve-2026.html
CISA Adds Actively Exploited SolarWinds Serv-U DoS Flaw to KEV Catalog	https://thehackernews.com/2026/06/cisa-adds-actively-exploited-solarwinds.html
Critical Everest Forms Pro flaw exploited to take over WordPress sites	https://www.bleepingcomputer.com/news/security/critical-everest-forms-pro-flaw-exploited-to-take-over-wordpress-sites/
Microsoft Edge Vulnerability Allows Remote Attackers to Execute Arbitrary Code	https://cybersecuritynews.com/microsoft-edge-vulnerability-code-execution/
Microsoft 365 Service Degradation Bypassed Windows Driver Auto-Update Controls	https://cybersecuritynews.com/microsoft-365-degradation-bypassed-windows-driver/
CISA Warns of Linux Kernel Improper Authentication Vulnerability Exploited in Attacks	HTTPS://CYBERSECURITYNEWS.COM/LINUX-KERNEL-IMPROPER-AUTHENTICATION-VULNERABILITY/
CISA Warns of SolarWinds Serv-U Vulnerability Exploited in Attacks	https://cybersecuritynews.com/cisa-solarwinds-serv-u-vulnerability/
21 0-Day Vulnerabilities in FFmpeg Enables Remote Code Execution Attacks	https://cybersecuritynews.com/21-0-day-vulnerabilities-in-ffmpeg/
Check Point VPN 0-day Vulnerability Exploited in the Wild to Deploy Ransomware	https://cybersecuritynews.com/check-point-vpn-0-day-vulnerability/
New Linux Kernel Vulnerability Lets Attackers Escalate Privileges to Root	https://cybersecuritynews.com/linux-kernel-nftables-vulnerability/
LiteLLM Flaw CVE-2026-42271 Exploited in the Wild, Chains to Unauthenticated RCE	https://thehackernews.com/2026/06/litellm-flaw-cve-2026-42271-exploited.html
Critical Check Point VPN Flaw Exploited to Bypass Passwords in IKEv1 Setups	https://thehackernews.com/2026/06/critical-check-point-vpn-flaw-exploited.html
Multiple VMware Stored XSS Vulnerabilities Allow Attackers to Inject Malicious Scripts	https://cybersecuritynews.com/vmware-stored-xss-vulnerabilities/

Patches / Updates / Fixes

Εδώ θα βρείτε τις πιο πρόσφατες διορθώσεις και ενημερώσεις ασφαλείας από προμηθευτές λογισμικού και hardware. Το περιεχόμενο αφορά συγκεκριμένα bugs ή exploits που έχουν ήδη δημοσιοποιηθεί, μαζί με οδηγίες για το πώς να εφαρμοστούν τα patches.

Σύντομη περιγραφή / Τίτλος	URL
AI Agent Uncovers 21 Zero-Days in FFmpeg; Chrome Patches Record 429 Bugs	https://thehackernews.com/2026/06/ai-agent-uncovers-21-zero-days-in.html
Let’s Encrypt Unveils Merkle Tree Certificates to Secure the Web Against Quantum Threats	https://cybersecuritynews.com/lets-encrypt-merkle-tree-certificates/
Instagram Fixes Password Reset Flaw That Exposes User Emails and Phone Numbers	https://cybersecuritynews.com/instagram-password-reset-user-phone/

New ChatGPT Lockdown Mode to Mitigate Prompt Injection and Data Exfiltration Attacks	https://cybersecuritynews.com/chatgpt-lockdown-mode/
Apache HTTP Server 2.4.68 Released With Fix For Use-After-Free, DoS, XSS, and Buffer Overflow Flaws	https://cybersecuritynews.com/apache-http-server-2-4-68/
Gogs patches critical zero-day enabling remote code execution	https://www.bleepingcomputer.com/news/security/gogs-patches-critical-zero-day-enabling-remote-code-execution/

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
Adaptive, Agentic AI Worms Loom as Next Enterprise Threat	https://www.darkreading.com/cyber-risk/adaptive-agentic-ai-worms-enterprise-cyber-threat
ClawHub, Cisco, Vercel's Malicious Skill Detector Bypassed to upload Malicious Skills	https://cybersecuritynews.com/clawhub-cisco-vercels-malicious-skill-detector-bypassed/
VECT 2.0 Ransomware Can Damage Files Its Own Decryptor Cannot Reliably Re-store	https://cybersecuritynews.com/vect-2-0-ransomware-can-damage-files-its-own-decryptor/
Chinese APT VerdantBamboo Uses BRICKSTORM Malware to Compromise Fire-walls and Appliances	https://cybersecuritynews.com/chinese-apt-verdantbamboo-uses-brickstorm-malware/
Malicious Browser Add-Ons Target ChatGPT, Claude, Copilot, Gemini, and DeepSeek Users	https://cybersecuritynews.com/malicious-browser-add-ons-target-chatgpt/
New SHub Stealer Variant Malware Targets Chrome, Firefox, Brave, Edge, Opera, and Crypto Wallets	https://cybersecuritynews.com/new-shub-stealer-variant-malware-targets-chrome/
New Gafgyt Variant Targets Multiple Linux Architectures With Modular Propaga-tion	https://cybersecuritynews.com/new-gafgyt-variant-targets-multiple-linux-architectures/
Hackers Can Hijack Claude Code MCP Traffic to Steal OAuth Tokens	https://cybersecuritynews.com/claude-code-mcp-traffic-hijack/
New EDRChoker Tool Uses Policy-Based Quality of Service to Block EDR Processes	https://cybersecuritynews.com/edrchoker-tool/
Hackers Publish Malicious Python Package Mimicking Legitimate Parsimonious Parser	https://cybersecuritynews.com/hackers-publish-malicious-python-package/
Hackers are Increasingly Weaponizing Trusted Tools to Deploy Notorious Malware	https://cybersecuritynews.com/hackers-are-increasingly-weaponizing-trusted-tools/
New China-Linked Threat Cluster OP-512 Targets IIS Servers With Cryptograph-ically Unique Web Shell Framework	https://cybersecuritynews.com/new-china-linked-threat-cluster-op-512-targets-iis-servers/
WhatsApp Disrupts NSO-Linked Cyberattack Targeting Users with Pegasus Spy-ware	https://cybersecuritynews.com/whatsapp-disrupts-nso-cyberattack/

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/