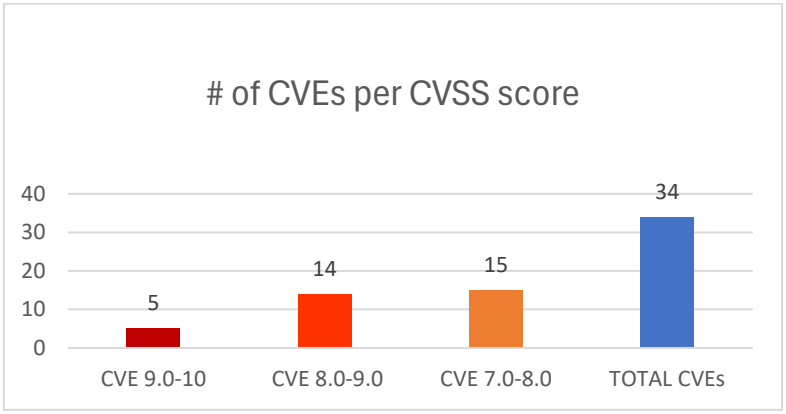
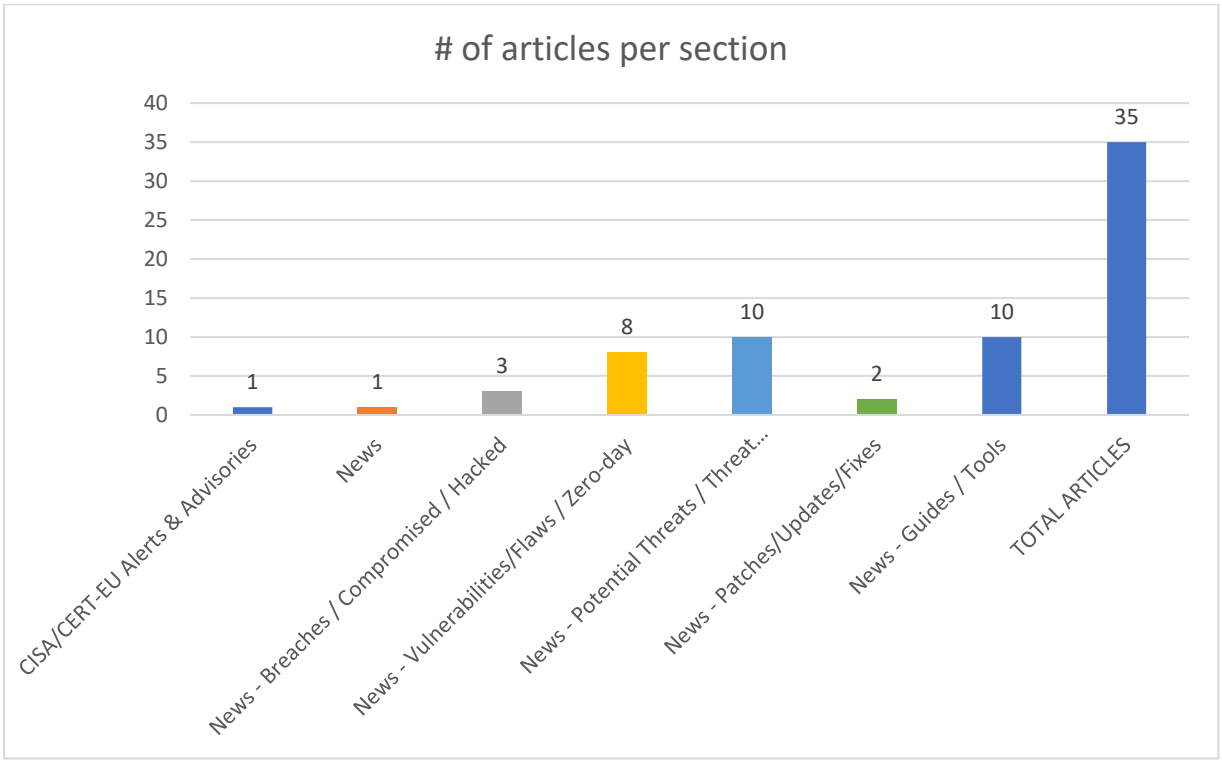
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 04/04/2026 - 07/04/2026





Contents

Common Vulnerabilities and Exposures (CVEs) 3
CISA/CERT-EU Alerts & Advisories 10
News 10
Breaches / Compromised / Hacked 11
Vulnerabilities / Flaws / Zero-day 11
Patches / Updates / Fixes 12
Potential threats / Threat intelligence 12
Guides / Tools 13
References 14
Annex – Websites with vendor specific vulnerabilities 15

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-2025-54328	10,0	Samsung	Stack-based Buffer Overflow	An issue was discovered in SMS in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, 2400, 1580, 2500, 9110, W920, W930, W1000, Modem 5123, Modem 5300, and Modem 5400	https://semiconductor.samsung.com/support/quality-support/product-security-updates/ https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2025-54328/
https://nvd.nist.gov/vuln/detail/CVE-2026-34208	10,0	SandboxJS	Protection Mechanism Failure	SandboxJS is a JavaScript sandboxing library. Prior to 0.8.36	https://github.com/nyariv/SandboxJS/security/advisories/GHSA-2gg9-6p7w-6cpj
https://nvd.nist.gov/vuln/detail/CVE-2026-34976	10,0	Dgraph	Missing Authorization	graph is an open source distributed GraphQL database. Prior to 25.3.1	https://github.com/dgraph-io/dgraph/security/advisories/GHSA-p5rh-vmhp-gvcw
https://nvd.nist.gov/vuln/detail/CVE-2026-35022	9,8	Anthropic Claude	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Anthropic Claude Code CLI and Claude Agent SDK	https://phoenix.security/critical-ci-cd-nightmare-3-command-injection-flaws-in-claude-code-cli-allow-credential-exfiltration/ https://www.vulncheck.com/advisories/anthropic-claude-code-agent-sdk-os-command-injection-via-authentication-helper
https://nvd.nist.gov/vuln/	9,1	GLPI	Improper Control of Generation of Code	GLPI is a free asset and IT management software package. From 11.0.0 to before 11.0.6, template injection by an	https://github.com/glpi-project/glpi/security/advisories/GHSA-2c98-648q-h27h

detail/CVE-2026-26026			('Code Injection')	administrator lead to RCE. This vulnerability is fixed in 11.0.6.	
https://nvd.nist.gov/vuln/detail/CVE-2026-3524	8,8	Mattermost	Missing Authorization	Mattermost Plugin Legal Hold versions <=1.1.4	https://mattermost.com/security-updates
https://nvd.nist.gov/vuln/detail/CVE-2026-5550	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda AC10 16.03.10.10_multi_TDE01	https://github.com/somanyerrors/tenda-ac10v4-vulnerabilities/blob/main/findings/HIGH-01-getvalue-229-callers.md https://vuldb.com/submit/782299 https://vuldb.com/vuln/355314 https://vuldb.com/vuln/355314/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-5566	8,8	UTT	Improper Restriction of Operations within the Bounds of a Memory Buffer	UTT HiPER 1250GW up to 3.2.7-210907-180535	https://github.com/Moxxkidd/CVE/issues/1 https://vuldb.com/submit/782993 https://vuldb.com/vuln/355336 https://vuldb.com/vuln/355336/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-5567	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda M3 1.0.0.10	https://github.com/Moxxkidd/CVE/issues/2 https://vuldb.com/submit/782999 https://vuldb.com/vuln/355337 https://vuldb.com/vuln/355337/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-5605	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda CH22 1.0.0.1	https://github.com/Litengzheng/vuldb_new/blob/main/CH22/vul_54/README.md https://vuldb.com/submit/785052 https://vuldb.com/vuln/355397 https://vuldb.com/vuln/355397/cti https://www.tenda.com.cn/

https://nvd.nist.gov/vuln/detail/CVE-2026-5609	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda i12 1.0.0.11(3862)	https://github.com/Li-tengzheng/vuldb_new/blob/main/i12/vul_107/README.md https://vuldb.com/submit/785337 https://vuldb.com/vuln/355400 https://vuldb.com/vuln/355400/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-5629	8,8	Belkin	Improper Restriction of Operations within the Bounds of a Memory Buffer	Belkin F9K1015 1.00.10	https://github.com/Li-tengzheng/vuldb_new/blob/main/Belkin%20F9K1015/vul_13/README.md https://vuldb.com/submit/785556 https://vuldb.com/vuln/355417 https://vuldb.com/vuln/355417/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-5686	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda CX12L 16.03.53.12	https://github.com/cve-a/lvdan/issues/4 https://vuldb.com/submit/792783 https://vuldb.com/vuln/355513 https://vuldb.com/vuln/355513/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-5687	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda CX12L 16.03.53.12	https://github.com/cve-a/lvdan/issues/5 https://vuldb.com/submit/792785 https://vuldb.com/vuln/355514 https://vuldb.com/vuln/355514/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-5707	8,8	OS command in the virtual desktop session name handling in AWS Research and	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	OS command in the virtual desktop session name handling in AWS Research and Engineering Studio (RES) version 2025.03 through 2025.12.01	https://aws.amazon.com/security/security-bulletins/2026-014-aws/ https://github.com/aws/res/issues/151 https://github.com/aws/res/releases/tag/2026.03

		Engineering Studio (RES)			
https://nvd.nist.gov/vuln/detail/CVE-2026-5708	8,8	AWS Research and Engineering Studio (RES)	Improperly Controlled Modification of Dynamically-Determined Object Attributes		https://aws.amazon.com/security/security-bulletins/2026-014-aws/ https://github.com/aws/res/issues/149 https://github.com/aws/res/releases/tag/2026.03
https://nvd.nist.gov/vuln/detail/CVE-2026-5709	8,8	FileBrowser API in AWS Research and Engineering Studio (RES)	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	FileBrowser API in AWS Research and Engineering Studio (RES) version 2024.10 through 2025.12.01	https://aws.amazon.com/security/security-bulletins/2026-014-aws/ https://github.com/aws/res/issues/150 https://github.com/aws/res/releases/tag/2026.03
https://nvd.nist.gov/vuln/detail/CVE-2026-34975	8,5	Plunk	Improper Neutralization of CRLF Sequences ('CRLF Injection')	Plunk is an open-source email platform built on top of AWS SES. Prior to 0.8.0	https://github.com/useplunk/plunk/security/advisories/GHSA-2mvm-rg5v-7hfq
https://nvd.nist.gov/vuln/detail/CVE-2026-34982	8,2	Vim	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Vim is an open source, command line text editor. Prior to version 9.2.0276	http://www.openwall.com/lists/oss-security/2026/04/01/1 https://github.com/vim/vim/commit/75661a66a1db1e1f3f1245c615 https://github.com/vim/vim/releases/tag/v9.2.0276 https://github.com/vim/vim/security/advisories/GHSA-8h6p-m6gr-mpw9

https://nvd.nist.gov/vuln/detail/CVE-2016-20056	7,8	Spy Emergency	Unquoted Search Path or Element	Spy Emergency build 23.0.205	http://www.spy-emergency.com/ http://www.spy-emergency.com/download/download.php?id=1 https://www.exploit-db.com/exploits/40550 https://www.vulncheck.com/advisories/spy-emergency-build-unquoted-service-path-privilege-escalation
https://nvd.nist.gov/vuln/detail/CVE-2016-20057	7,8	NETGATE Registry Cleaner	Unquoted Search Path or Element	NETGATE Registry Cleaner build 16.0.205	http://www.netgate.sk/ http://www.netgate.sk/download/download.php?id=4 https://www.exploit-db.com/exploits/40539 https://www.vulncheck.com/advisories/netgate-registry-cleaner-build-unquoted-service-path-privilege-escalation
https://nvd.nist.gov/vuln/detail/CVE-2016-20058	7,8	Netgate AMITI Antivirus	Unquoted Search Path or Element	Netgate AMITI Antivirus	http://www.netgate.sk/ http://www.netgate.sk/download/download.php?id=11 https://www.exploit-db.com/exploits/40540 https://www.vulncheck.com/advisories/netgate-amiti-antivirus-build-unquoted-service-path-privilege-escalation
https://nvd.nist.gov/vuln/detail/CVE-2016-20060	7,8	Hotspot Shield	Unquoted Search Path or Element	Hotspot Shield 6.0.3	https://www.exploit-db.com/exploits/40528 https://www.hotspotshield.com https://www.hotspotshield.com/download/ https://www.vulncheck.com/advisories/hotspot-shield-unquoted-service-path-privilege-escalation
https://nvd.nist.gov/vuln/detail/CVE-2024-14032	7,8	Twitch Studio	Missing Authorization	Twitch Studio version 0.114.8 and prior	https://help.twitch.tv/s/article/recommended-software-for-broadcasting https://help.twitch.tv/s/topic/0TO3a000000kZfYGAU/twitch-studio https://www.iru.com/blog/twitch-privileged-helper

					https://www.vulncheck.com/advisories/twitch-studio-launcherhelper-xpc-missing-authorization-to-root-file-write
https://nvd.nist.gov/vuln/detail/CVE-2026-35021	7,8	Anthropic Claude	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Anthropic Claude Code CLI and Claude Agent SDK contain an OS command injection	https://phoenix.security/critical-ci-cd-nightmare-3-command-injection-flaws-in-claude-code-cli-allow-credential-exfiltration/ https://www.vulncheck.com/advisories/anthropic-claude-code-agent-sdk-os-command-injection-via-prompteditor-ts
https://nvd.nist.gov/vuln/detail/CVE-2026-34986	7,5	Go JOSE	Uncaught Exception	Go JOSE provides an implementation of the Javascript Object Signing and Encryption set of standards in Go, including support for JSON Web Encryption (JWE), JSON Web Signature (JWS), and JSON Web Token (JWT) standards. Prior to 4.1.4 and 3.0.5	https://github.com/go-jose/go-jose/security/advisories/GHSA-78h2-9frx-2jm8 https://pkg.go.dev/github.com/go-jose/go-jose/v4#pkg-constants
https://nvd.nist.gov/vuln/detail/CVE-2026-5526	7,3	Tenda	Incorrect Privilege Assignment	Tenda 4G03 Pro up to 1.0/1.1/04.03.01.53/192.168.0.1	https://vuldb.com/submit/782052 https://vuldb.com/vuln/355279 https://vuldb.com/vuln/355279/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-5562	7,3	kafka	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	kafka-ui up to 0.7.2	https://drive.google.com/file/d/18-Q4tb19y_7dwchnTCgcwfbox0Uj6oQd/view https://vuldb.com/submit/782941 https://vuldb.com/vuln/355332 https://vuldb.com/vuln/355332/cti
https://nvd.nist.gov/vuln/	7,3	Totolink	Improper Authentication	Totolink A8000R 5.9c.681_B20180413	https://github.com/skeetabc/CVE-TOTOLINK-A800R/blob/main/vuln1_auth_bypass.md VulDB https://vuldb.com/submit/792433 VulDB

detail/CVE-2026-5676					https://vuldb.com/vuln/355503 VulDB https://vuldb.com/vuln/355503/cti VulDB https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-5678	7,3	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink A7100RU 7.4cu.2313_b20191024	https://github.com/Li-tengzheng/vuldb_new/blob/main/A7100RU/vul_185/README.md https://vuldb.com/submit/792608 https://vuldb.com/vuln/355505 https://vuldb.com/vuln/355505/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-5689	7,3	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink A7100RU 7.4cu.2313_b20191024	https://github.com/Li-tengzheng/vuldb_new/blob/main/A7100RU/vul_187/README.md https://vuldb.com/submit/792946 https://vuldb.com/vuln/355516 https://vuldb.com/vuln/355516/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-5690	7,3	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink A7100RU 7.4cu.2313_b20191024	https://github.com/Li-tengzheng/vuldb_new/blob/main/A7100RU/vul_188/README.md https://vuldb.com/submit/792947 https://vuldb.com/vuln/355517 https://vuldb.com/vuln/355517/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-5691	7,3	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink A7100RU 7.4cu.2313_b20191024	https://github.com/Li-tengzheng/vuldb_new/blob/main/A7100RU/vul_189/README.md https://vuldb.com/submit/792962 https://vuldb.com/vuln/355518 https://vuldb.com/vuln/355518/cti https://www.totolink.net/

https://nvd.nist.gov/vuln/detail/CVE-2026-29047	7,2	GLPI	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	GLPI is a free asset and IT management software package. From 10.0.0 to before 10.0.24 and 11.0.6, an authenticated user can perform a SQL injection via the logs export feature. This vulnerability is fixed in 10.0.24 and 11.0.6.	https://github.com/glpi-project/glpi/security/advisories/GHSA-3m49-qf92-vccr

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-2026-35616 - Fortinet FortiClient EMS Improper Access Control Vulnerability**	**https://www.cisa.gov/news-events/alerts/2026/04/06/cisa-adds-one-known-exploited-vulnerability-catalog**

News

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

Σύντομη περιγραφή / Τίτλος	URL
Anthropic Officially Ends Claude Subscriptions for Third-Party Tools Like OpenClaw	https://cybersecuritynews.com/claude-ends-openclaw-subscriptions/

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
50,000 WordPress Sites Exposed to Critical Ninja Forms File Upload RCE Vulnerability	https://cybersecuritynews.com/50000-wordpress-sites-exposed/
Hackers Compromised ILSpy WordPress Domain to Deliver Malware	https://cybersecuritynews.com/ilspy-wordpress-domain-malware/
2,000+ FortiClient EMS Instances Exposed Online Amid Active RCE Vulnerability Exploits in the Wild	https://cybersecuritynews.com/forticlient-ems-instances-exposed-online/

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
New FortiClient EMS flaw exploited in attacks, emergency patch released	https://www.bleepingcomputer.com/news/security/new-fortinet-forticlient-ems-flaw-cve-2026-35616-exploited-in-attacks/
China-Linked Storm-1175 Exploits Zero-Days to Rapidly Deploy Medusa Ransomware	https://thehackernews.com/2026/04/china-linked-storm-1175-exploits-zero.html
Flowise AI Agent Builder Under Active CVSS 10.0 RCE Exploitation; 12,000+ Instances Exposed	https://thehackernews.com/2026/04/flowise-ai-agent-builder-under-active.html
OpenAI Codex Command Injection Vulnerability Let Attackers Steal GitHub User Access Tokens	https://cybersecuritynews.com/openai-codex-command-injection-vulnerability/
CISA Warns of Fortinet 0-Day Vulnerability Actively Exploited in Attacks	https://cybersecuritynews.com/cisa-warns-fortinet-vulnerability/
Apache Traffic Server Vulnerabilities Let Attackers Trigger DoS Attack	https://cybersecuritynews.com/apache-traffic-server-dos-vulnerabilities/
Critical Dgraph Database Vulnerability Let Attackers Bypass Authentication	https://cybersecuritynews.com/dgraph-database-vulnerability/
CISA Adds TrueConf Vulnerability to KEV Catalog Following Active Exploitation	https://cybersecuritynews.com/cisa-trueconf-vulnerability-kev-catalog/

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
Fortinet Patches Actively Exploited CVE-2026-35616 in FortiClient EMS	https://thehackernews.com/2026/04/fortinet-patches-actively-exploited-cve.html
CISA orders feds to patch exploited Fortinet EMS flaw by Friday	https://www.bleepingcomputer.com/news/security/cisa-orders-feds-to-patch-fortinet-flaw-exploited-in-attacks-by-friday/

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
Hackers Use Fake TradingView Premium Posts on Reddit to Deliver Vidar and AMOS Stealers	https://cybersecuritynews.com/hackers-use-fake-tradingview-premium-posts/
Trojanized PyPI AI Proxy Uses Stolen Claude Prompt to Exfiltrates Data	https://cybersecuritynews.com/trojanized-pypi-ai-proxy-uses-stolen-claude-prompt/
Hackers Use Poisoned Axios Package and Phantom Dependency to Spread Cross-Platform Malware	https://cybersecuritynews.com/hackers-use-poisoned-axios-package-and-phantom-dependency/
Hackers Using Fake "Microsoft Teams" Domains to Attack Users Via Malicious Payload	https://cybersecuritynews.com/hackers-using-fake-microsoft-teams-domains-attack-via-malicious-payload/
Google DeepMind Researchers Warn Hackers Can Hijack AI Agents Through Malicious Web Content	https://cybersecuritynews.com/hackers-hijack-ai-agents/
Researcher Released Windows Defender 0-Day Exploit Code, Allowing Attackers to Gain Full Access	https://cybersecuritynews.com/windows-defender-0-day-exploit/
New GitHub Actions Attack Chain Uses Fake CI Updates to Exfiltrate Secrets and Tokens	https://cybersecuritynews.com/new-github-actions-attack-chain-uses-fake-ci-updates/
DPRK Cyber Program Uses Modular Malware Strategy to Evade Attribution and Survive Takedowns	https://cybersecuritynews.com/dprk-cyber-program-uses-modular-malware-strategy/
Hackers Weaponize Claude Code Leak to Spread Vidar and GhostSocks Malware	https://cybersecuritynews.com/claude-code-leak-to-spread-vidar-and-ghostsocks-malware/
Top Node.js Maintainers Targeted in Sophisticated Social Engineering Scheme	https://cybersecuritynews.com/top-node-js-maintainers-targeted-social-engineering-scheme/

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

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/