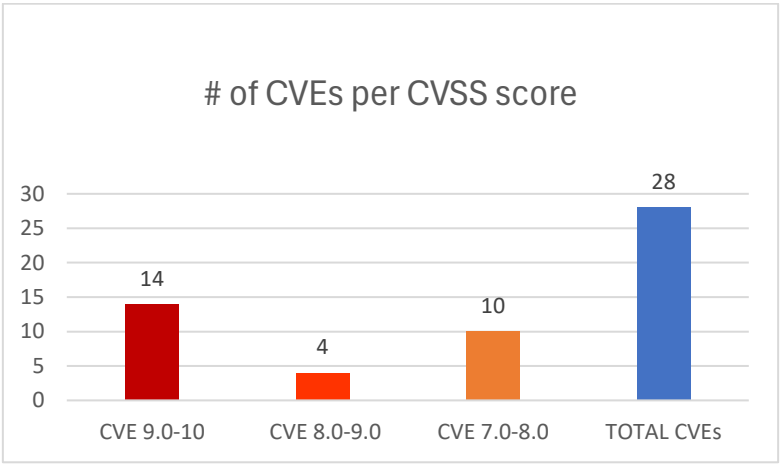
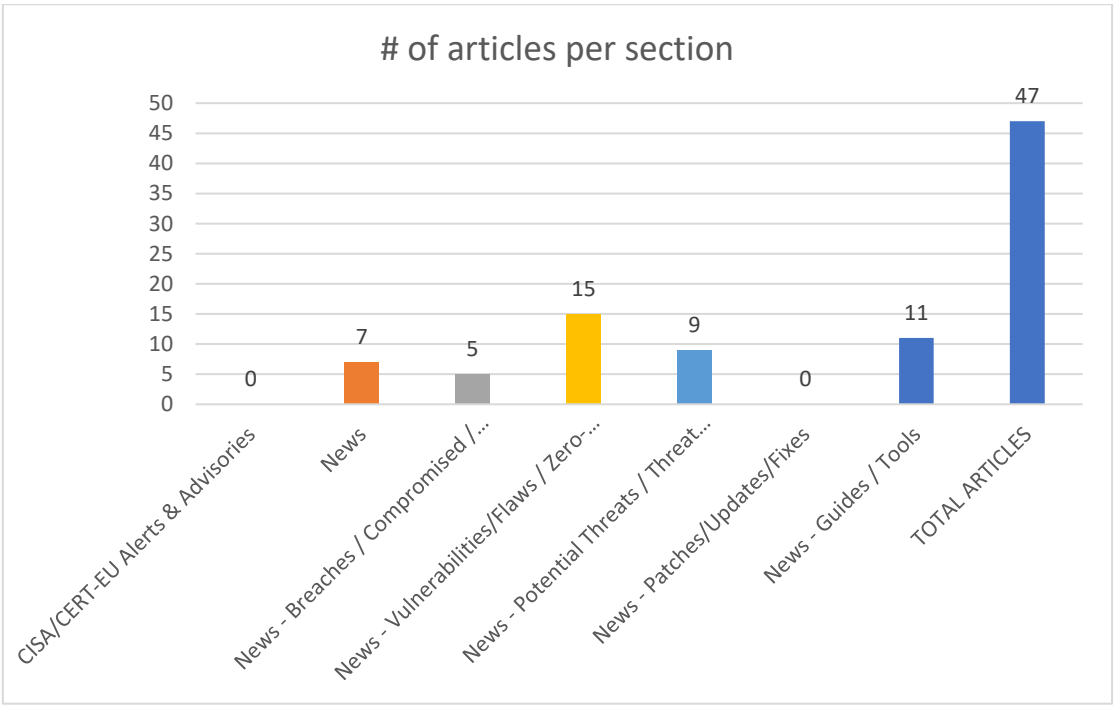
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 25/04/2026 - 28/04/2026





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-2026-33453	10,0	Apache Camel Camel-Coap	Improperly Controlled Modification of Dynamically-Determined Object Attributes	This issue affects Apache Camel: from 4.14.0 through 4.14.5, from 4.18.0 before 4.18.1, 4.19.0. Users are recommended to upgrade to version 4.18.1 or 4.19.0, fixing the issue	http://www.openwall.com/lists/oss-security/2026/04/26/3 https://camel.apache.org/security/CVE-2026-33453.html
https://nvd.nist.gov/vuln/detail/CVE-2026-21515	9,9	Azure IOT Central	Exposure of Sensitive Information to an Unauthorized Actor	-	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21515
https://nvd.nist.gov/vuln/detail/CVE-2026-1952	9,8	Delta Electronics	Hidden Functionality	Delta Electronics AS320T	https://filecenter.deltaww.com/news/download/doc/Delta-PCSA-2026-00006_AS320T%20Multiple%20vulnerabilities%20(CVE-2026-1949,%201950,%201951,%201952).pdf
https://nvd.nist.gov/vuln/detail/CVE-2026-32644	9,8	Milesight AIOT	Use of Hard-coded Cryptographic Key	-	https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-113-03.json https://www.cisa.gov/news-events/ics-advisories/icsa-26-113-03 https://www.milesight.com/support/download/firmware
https://nvd.nist.gov/vuln/detail/CVE-2026-41492	9,8	Dgraph	Exposure of Sensitive Information to an Unauthorized Actor	Prior to 25.3.3	https://github.com/dgraph-io/dgraph/releases/tag/v25.3.3 https://github.com/dgraph-io/dgraph/security/advisories/GHSA-vvf7-6rmr-m29q

https://nvd.nist.gov/vuln/detail/CVE-2026-41635	9,8	Apache MINA	Deserialization of Untrusted Data	Affected versions are Apache MINA 2.0.0 <= 2.0.27, 2.1.0 <= 2.1.10, and 2.2.0 <= 2.2.5. The problem is resolved in Apache MINA 2.0.28, 2.1.11, and 2.2.6	http://www.openwall.com/lists/oss-security/2026/04/27/4 https://lists.apache.org/thread/1l91w1mqsb3lwfd504fs045ylxntt2tm
https://nvd.nist.gov/vuln/detail/CVE-2026-6911	9,8	AWS Ops Wheel	Improper Verification of Cryptographic Signature	-	https://aws.amazon.com/security/security-bulletins/2026-018-aws/ https://github.com/aws/aws-ops-wheel/pull/164 https://github.com/aws/aws-ops-wheel/security/advisories/GHSA-v5vr-8w3c-37x2
https://nvd.nist.gov/vuln/detail/CVE-2026-7204	9,8	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink A8000RU 7.1cu.643_b20200521	https://github.com/Litengzheng/vuldb_new2/blob/main/A8000RU/vul_323/README.md https://vuldb.com/vuln/359804 https://vuldb.com/vuln/359804/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-31685	9,4	Linux kernel	-	In the Linux kernel, the following vulnerability has been resolved: netfilter: ip6t_eui64: reject invalid MAC header for all packets `eui64_mt6()` derives a modified EUI-64 from the Ethernet source address and compares it with the low 64 bits of the IPv6 source address.	https://git.kernel.org/stable/c/288138418bef956f8b295751a4536c60f0e89f4a https://git.kernel.org/stable/c/309ae3e9a51a69699ca94eac5fac5688fa562d55 https://git.kernel.org/stable/c/807d6ee15804df6f01a35c910f09612e858739a6 https://git.kernel.org/stable/c/9eda5478746ef7dc0e4e537b5a5e4b0ca1027091 https://git.kernel.org/stable/c/fdce0b3590f724540795b874b4c8850c90e6b0a8
https://nvd.nist.gov/vuln/detail/CVE-2026-33454	9,4	Camel-Mail	Deserialization of Untrusted Data	This issue affects Apache Camel: from 3.0.0 before 4.14.6, from 4.15.0 before 4.18.1. Users are recommended to up-	https://camel.apache.org/security/CVE-2026-33454.html

				grade to version 4.19.0, which fixes the issue. If users are on the 4.18.x LTS releases stream, then they are suggested to upgrade to 4.18.1. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.6	
https://nvd.nist.gov/vuln/detail/CVE-2026-31682	9,1	Linux kernel	-	In the Linux kernel, the following vulnerability has been resolved: bridge: br_nd_send	https://git.kernel.org/stable/c/2ba4caba423ed94d63006eb1d2227b0332ab7fcd kernel.org https://git.kernel.org/stable/c/3a30f6469b058574f49efde61cd6f5d79e576053 kernel.org https://git.kernel.org/stable/c/4f397b950c916e9a1f8a4fce04ea0110206cad47 kernel.org https://git.kernel.org/stable/c/658261898130da620fc3d0fbb0523efb3366cb55 https://git.kernel.org/stable/c/9c55e41c73af5c4511070933b1bd25248521270c https://git.kernel.org/stable/c/a01aee7cafc575bb82f5529e8734e7052f9b16ea https://git.kernel.org/stable/c/bd91ec85aa4c77d645bd2739fc56784157a88ca2 https://git.kernel.org/stable/c/c68433fd291c9e88c00292095172c62d1997d662
https://nvd.nist.gov/vuln/detail/CVE-2026-40976	9,1	Spring Boot	Missing Authorization	Affected: Spring Boot 4.0.0–4.0.5; upgrade to 4.0.6 or later per vendor advisory	https://spring.io/security/cve-2026-40976

https://nvd.nist.gov/vuln/detail/CVE-2026-41248	9,1	Clerk JavaScript	Interpretation Conflict	This vulnerability is fixed in @clerk/astro 1.5.7, 2.17.10, and 3.0.15; @clerk/nextjs 5.7.6, 6.39.2, and 7.2.1; @clerk/nuxt 1.13.28 and 2.2.2; and @clerk/shared 2.22.1, 3.47.4, anc 4.8.1	https://github.com/clerk/javascript/security/advisories/GHSA-vqx2-fgx2-5wq9
https://nvd.nist.gov/vuln/detail/CVE-2026-42044	9,1	Axios	Improperly Controlled Modification of Dynamically-Determined Object Attributes	From 1.0.0 to before 1.15.2	https://github.com/axios/axios/security/advisories/GHSA-3w6x-2g7m-8v23
https://nvd.nist.gov/vuln/detail/CVE-2026-7082	8,8	Tenda	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	F456 1.0.0.5	https://github.com/Litengzheng/vuldb_new/blob/main/F456/vul_134/README.md VulDB https://vuldb.com/submit/798465 VulDB https://vuldb.com/vuln/359657 VulDB https://vuldb.com/vuln/359657/cti VulDB https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-7160	8,8	Tenda	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	HG3 2.0	https://vuldb.com/submit/802079 VulDB https://vuldb.com/vuln/359759 VulDB https://vuldb.com/vuln/359759/cti VulDB https://www.notion.so/33e0c75766a880488924cf24523acf6c VulDB https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-40967	8,6	Spring AI	Improper Control of Generation of Code ('Code Injection')	1.0.0 - 1.0.5 (fixed in 1.0.6), 1.1.0 - 1.1.4 (fixed in 1.1.5)	https://spring.io/security/cve-2026-40967
https://nvd.nist.gov/vuln/detail/CVE-2026-41364	8,1	OpenClaw	Improper Link Resolution Before File Access ('Link Following')	before 2026.3.31	https://github.com/openclaw/openclaw/commit/3d5af14984ac1976c747a8e11581d697bd0829dc VulnCheck https://github.com/openclaw/openclaw/security/advisories/GHSA-fv94-qvg8-xqpw VulnCheck https://www.vulncheck.com/advisories/openclaw-

					arbitrary-file-write-via-symlink-following-in-ssh-sandbox-tar-upload
https://nvd.nist.gov/vuln/detail/CVE-2026-40972	7,5	Spring Boot	Observable Timing Discrepancy	4.0.0–4.0.5 (fix 4.0.6), 3.5.0–3.5.13 (fix 3.5.14), 3.4.0–3.4.15 (fix 3.4.16), 3.3.0–3.3.18 (fix 3.3.19), 2.7.0–2.7.32 (fix 2.7.33)	https://spring.io/security/cve-2026-40972
https://nvd.nist.gov/vuln/detail/CVE-2026-7237	7,3	AgiFlow	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	up to 1.0.27	https://github.com/AgiFlow/aicode-toolkit/commit/c4d23592ae5fb59cfeefc4641e6826f8ac89b9c6 VulDB https://github.com/AgiFlow/aicode-toolkit/issues/88 VulDB https://github.com/AgiFlow/aicode-toolkit/pull/89 VulDB https://github.com/AgiFlow/aicode-toolkit/releases/tag/%40agiflowai/aicode-toolkit%401.1.0 VulDB https://vuldb.com/submit/802836 VulDB https://vuldb.com/vuln/359845 VulDB https://vuldb.com/vuln/359845/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-7228	7,3	SourceCodester Pizzafy Ecommerce System	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	1.0	https://github.com/fernando-mengali/vulndb-submissions/blob/main/05-vul-SQLI.md VulDB https://vuldb.com/submit/802416 VulDB https://vuldb.com/vuln/359828 VulDB https://vuldb.com/vuln/359828/cti VulDB https://www.sourcecodester.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-7177	7,3	ChatGPTNextWeb	Server-Side Request Forgery (SSRF)	up to 2.16.1	https://gist.github.com/YLChen-007/da6b00024f5b7e1d4fa0658c19b77fbf VulDB https://github.com/ChatGPTNextWeb/NextChat/ VulDB https://github.com/ChatGPT-NextWeb/NextChat/issues/6742 VulDB https://vuldb.com/submit/797645 VulDB https://vuldb.com/vuln/359779 VulDB https://vuldb.com/vuln/359779/cti

https://nvd.nist.gov/vuln/detail/CVE-2026-7194	7,3	Source-Codester Pharmacy Sales and Inventory System	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	1.0	https://github.com/bfs045313-wq/cv3-protect/issues/2 VulDB https://vuldb.com/submit/800977 VulDB https://vuldb.com/vuln/359798 VulDB https://vuldb.com/vuln/359798/cti VulDB https://www.sourcecodester.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-7221	7,3	TencentCloudBase	Server-Side Request Forgery (SSRF)	up to 2.17.0	https://github.com/TencentCloudBase/Cloud-Base-MCP/ VulDB https://github.com/TencentCloudBase/Cloud-Base-MCP/commit/3f678a1e7bd400cd76469d61024097d4920dc6b5 VulDB https://github.com/TencentCloudBase/Cloud-Base-MCP/issues/509 VulDB https://github.com/TencentCloudBase/Cloud-Base-MCP/pull/510 VulDB https://github.com/TencentCloudBase/Cloud-Base-MCP/releases/tag/v2.17.1 VulDB https://vuldb.com/submit/802230 VulDB https://vuldb.com/vuln/359821 VulDB https://vuldb.com/vuln/359821/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-7223	7,3	BigSweetPotatoStudio HyperChat	Server-Side Request Forgery (SSRF)	up to 2.0.0-alpha.63	https://github.com/BigSweetPotatoStudio/HyperChat/ VulDB https://github.com/BigSweetPotatoStudio/HyperChat/issues/142 VulDB https://vuldb.com/submit/802265 VulDB https://vuldb.com/vuln/359823 VulDB https://vuldb.com/vuln/359823/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-7213	7,3	ef10007 MLOps_MCP	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	1.0.0	https://github.com/ef10007/MLOps_MCP/ VulDB https://github.com/ef10007/MLOps_MCP/issues/1 VulDB https://vuldb.com/submit/802085 VulDB

					https://vuldb.com/vuln/359809 VulDB https://vuldb.com/vuln/359809/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-7218	7,2	Totolink	Improper Restriction of Operations within the Bounds of a Memory Buffer	N300RT 3.4.0-B20250430	https://github.com/xiaohaiyang-ai/TOTOLINK-N300RT-Buffer-Overflow VulDB https://vuldb.com/submit/802127 VulDB https://vuldb.com/vuln/359818 VulDB https://vuldb.com/vuln/359818/cti VulDB https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-1460	7,2	Zyxel DX3301-T0 and EX3301-T0 firmware	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	through 5.50(ABVY.7.1)C0	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-vulnerabilities-in-certain-4g-lte-5g-nr-cpe-dsl-ethernet-cpe-fiber-onts-and-wireless-extenders-04-28-2026

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
Parsing Agentic Offensive Security's Existential Threat	https://www.darkreading.com/cyber-risk/industrialized-exploitation-agentic-offensive-security-existential-threat
Utilities Tech Supplier Itron Discloses Cyber-Attack, Operations Unaffected	https://www.infosecurity-magazine.com/news/utilities-tech-supplier-itron/
US Sanctions Target Cambodian Scam Network Leaders	https://www.infosecurity-magazine.com/news/us-sanctions-cambodian-scam-network/

Researchers Warn macOS textutil and KeePassXC Can Become Attack Primitives in Automation	https://cybersecuritynews.com/researchers-warn-macos-textutil-and-keepassxc/
EU Proposes Requiring Google to Share User Search Data with Rival Search Engines	https://cybersecuritynews.com/eu-proposes-google-search-data/
Microsoft Officially Shares Group Policy to Remove Windows 11 Copilot from Enterprise Devices	https://cybersecuritynews.com/windows-11-copilot-remove/
GPT-5.5 Bio Bug Bounty to Strengthen Advanced AI Capabilities	https://cybersecuritynews.com/gpt-5-5-bio-bug-bounty/

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
Microsoft Confirms Active Exploitation of Windows Shell CVE-2026-32202	https://thehackernews.com/2026/04/microsoft-confirms-active-exploitation.html
PhantomCore Exploits TrueConf Vulnerabilities to Breach Russian Networks	https://thehackernews.com/2026/04/phantomcore-exploits-trueconf.html
ClickUp's Hardcoded API Key Exposes 959 Emails from Fortune 500 Giants	https://cybersecuritynews.com/clickup-hardcoded-api-key-expose/
New Vidar Malware Campaign Uses Fake YouTube Software Downloads to Steal Corporate Credentials	https://cybersecuritynews.com/new-vidar-malware-uses-fake-youtube-software-downloads/
ADT Confirms Data Breach Following ShinyHunters Data Leak Claim	https://cybersecuritynews.com/adt-confirms-data-breach/

Vulnerabilities / Flaws / Zero-day

Αναφέρονται τεχνικά ελαττώματα ή αδυναμίες που ενδέχεται να αξιοποιηθούν άμεσα από επιτιθέμενους — είτε επειδή είναι zero-day είτε γιατί η διόρθωσή τους καθυστερεί. Περιλαμβάνονται περιπτώσεις όπου δεν απαιτείται αλληλεπίδραση με τον χρήστη ή όπου παρακάμπτονται βασικά μέτρα ασφαλείας. Πολύ χρήσιμο για ομάδες που ασχολούνται με threat detection.

Σύντομη περιγραφή / Τίτλος	URL
Incomplete Windows Patch Opens Door to Zero-Click Attacks	https://www.securityweek.com/incomplete-windows-patch-opens-door-to-zero-click-attacks/
OpenSSH Flaw Allowing Full Root Shell Access Lurked for 15 Years	https://www.securityweek.com/openssh-flaw-allowing-full-root-shell-access-lurked-for-15-years/
Easily Exploitable 'Pack2TheRoot' Linux Vulnerability Leads to Root Access	https://www.securityweek.com/easily-exploitable-pack2theroot-linux-vulnerability-leads-to-root-access/
Firefox Vulnerability Allows Tor User Fingerprinting	https://www.securityweek.com/firefox-vulnerability-allows-tor-user-fingerprinting/
Unpatched 'PhantomRPC' Flaw in Windows Enables Privilege Escalation	https://www.darkreading.com/vulnerabilities-threats/unpatched-phantomrpc-flaw-windows-privilege-escalation

Notepad++ Vulnerability Allows Attackers to Crash Application, Leak Memory Data	https://cybersecuritynews.com/notepad-vulnerability-crash/
Critical Gemini CLI Vulnerability Enables Remote Code Execution Attacks	https://cybersecuritynews.com/gemini-cli-rce-vulnerability/
Microsoft Outlook.com Issue Blocks Users From Accessing Emails	https://cybersecuritynews.com/microsoft-outlook-com-issue-blocks-users/
Attackers Can Backdoor CODESYS Applications by Chaining Vulnerabilities	https://cybersecuritynews.com/attackers-backdoor-codesys-applications/
Nessus Agent Vulnerability on Windows Enables Arbitrary Code Execution with SYSTEM Privileges	https://cybersecuritynews.com/nessus-agent-vulnerability-on-windows/
Litecoin Zero-Day Vulnerability Exploited in DoS Attack, Disrupts Major Mining Pools	https://cybersecuritynews.com/litecoin-zero-day-vulnerability-exploited/
New Windows RPC Vulnerability Lets Attackers Escalate Privileges Across All Windows Versions	https://cybersecuritynews.com/new-windows-rpc-vulnerability/
CISA Warns of Multiple SimpleHelp Vulnerabilities Exploited in Attack	https://cybersecuritynews.com/simplehelp-vulnerabilities-exploited/
Hackers Can Abuse Entra Agent ID Administrator Role to Hijack Service Principals	https://cybersecuritynews.com/entra-agent-id-administrator-abused/
Hackers Exploiting Cisco Firepower Devices' Using n-day Vulnerabilities to Gain Unauthorized Access	https://cybersecuritynews.com/hackers-exploiting-cisco-firepower-devices-using-n-day-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

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
Widely Used Browser Extensions Selling User Data	https://www.infosecurity-magazine.com/news/browser-extensions-sell-user-data/
Fake Document Reader On Google Play With 10K Downloads Installing Anatsa Malware	https://cybersecuritynews.com/fake-document-reader-on-google-play/
AI Coding Agent Powered by Claude Opus 4.6 Deletes Production Database in 9 Seconds	https://cybersecuritynews.com/ai-coding-agent-deletes-data/
New Vidar Malware Campaign Uses Fake YouTube Software Downloads to Steal Corporate Credentials	https://cybersecuritynews.com/new-vidar-malware-uses-fake-youtube-software-downloads/
New Malware Uses Obfuscation and Staged Payload Delivery to Evade Detection	https://cybersecuritynews.com/new-malware-uses-obfuscation-and-staged-payload/

North Korean Hackers Attacking Drug Companies to Deploy Malware Via Weaponized Excel Files	https://cybersecuritynews.com/north-korean-hackers-attacking-drug-companies/
ClickFix Attack Replaces PowerShell With Cmdkey and Remote Regsvr32 Payload Delivery	https://cybersecuritynews.com/clickfix-attack-replaces-powershell-with-cmdkey/
Vidar Malware Hides Second-Stage Payloads in JPEG and TXT Files to Evade Detection	https://cybersecuritynews.com/vidar-malware-hides-second-stage-payloads-in-jpeg-and-txt-files/
73 Open VSX Sleeper Extensions Linked to GlassWorm Activate New Malware Campaign	https://cybersecuritynews.com/73-open-vsx-sleeper-extensions-linked-to-glassworm-malware/

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

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/