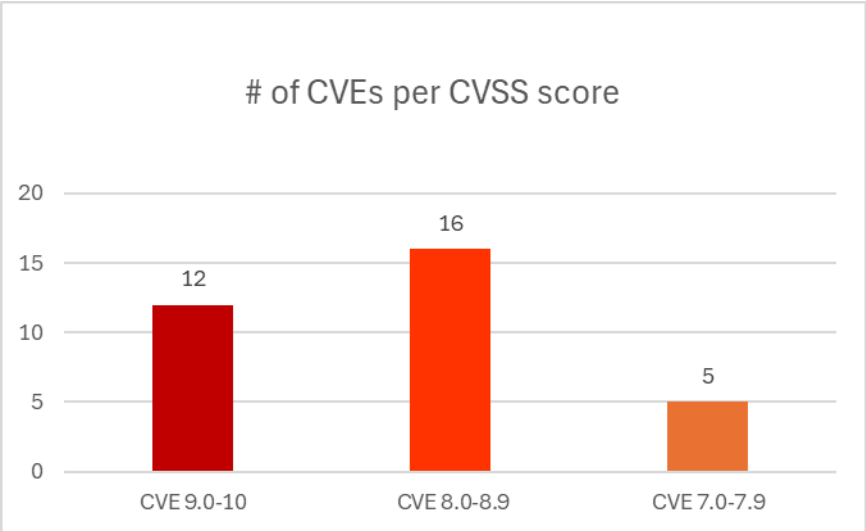
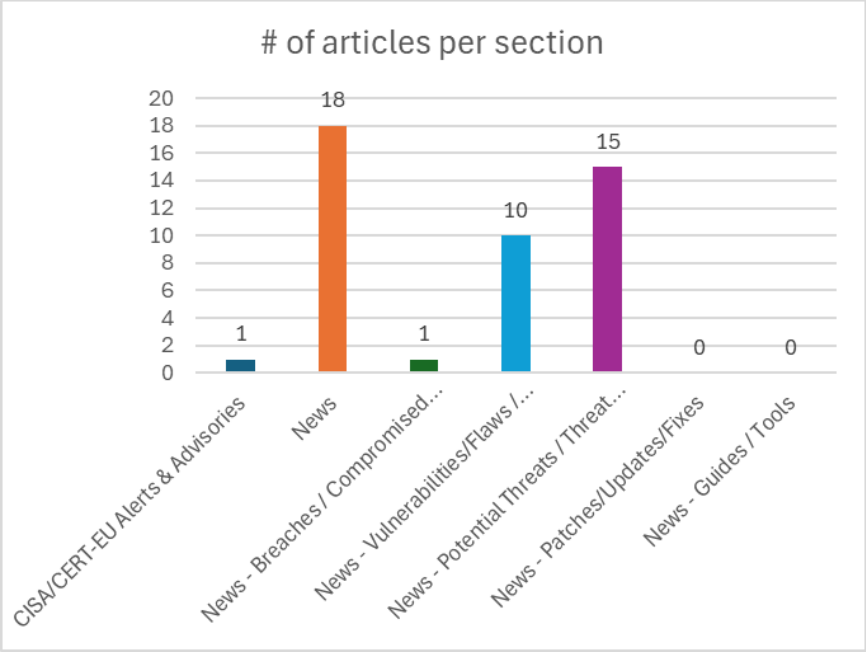
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 11/04/2026 - 14/04/2026





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-2026-6115	9,8	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink A7100RU 7.4cu.2313_b20191024	https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_180/README.md https://vuldb.com/submit/792248 https://vuldb.com/vuln/356975 https://vuldb.com/vuln/356975/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-6116	9,8	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink A7100RU 7.4cu.2313_b20191024	https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_181/README.md https://vuldb.com/submit/792249 https://vuldb.com/vuln/356976 https://vuldb.com/vuln/356976/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-6131	9,8	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink A7100RU 7.4cu.2313_b20191024	https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_182/README.md https://vuldb.com/submit/792251 https://vuldb.com/vuln/356995 https://vuldb.com/vuln/356995/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-6132	9,8	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink A7100RU 7.4cu.2313_b20191024	https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_183/README.md https://vuldb.com/submit/792252 https://vuldb.com/vuln/356996 https://vuldb.com/vuln/356996/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-6139	9,8	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink A7100RU 7.4cu.2313_b20191024	https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_192/README.md https://vuldb.com/submit/792982 https://vuldb.com/vuln/357003 https://vuldb.com/vuln/357003/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-6140	9,8	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink A7100RU 7.4cu.2313_b20191024	https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_193/README.md https://vuldb.com/submit/792987 https://vuldb.com/vuln/357004

					https://vuldb.com/vuln/357004/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-6154	9,8	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink A7100RU 7.4cu.2313_b20191024	https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_194/README.md https://vuldb.com/submit/792990 https://vuldb.com/vuln/357034 https://vuldb.com/vuln/357034/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-6155	9,8	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink A7100RU 7.4cu.2313	https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_196/README.md https://vuldb.com/submit/793679 https://vuldb.com/vuln/357035 https://vuldb.com/vuln/357035/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-6156	9,8	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink A7100RU 7.4cu.2313_b20191024	https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_197/README.md https://vuldb.com/submit/793681 https://vuldb.com/vuln/357036 https://vuldb.com/vuln/357036/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-6195	9,8	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink A7100RU 7.4cu.2313_b20191024	https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_198/README.md https://vuldb.com/submit/797460 https://vuldb.com/vuln/357117 https://vuldb.com/vuln/357117/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-33707	9,4	Chamilo LMS	Weak Password Recovery Mechanism for Forgotten Password	Prior to 1.11.38 and 2.0.0-RC.3	https://github.com/chamilo/chamilo-lms/commit/078d7e5b77679fa7ccfcd6783bd5cc683db0bda8 https://github.com/chamilo/chamilo-lms/commit/750a45312a0d5c3ad60dbfbd0d959ca40be4a18c https://github.com/chamilo/chamilo-lms/security/advisories/GHSA-f27g-66gq-g7v2
https://nvd.nist.gov/vuln/detail/CVE-2026-35652	9,1	OpenClaw	Incorrect Behavior Order	OpenClaw before 2026.3.22	https://github.com/openclaw/openclaw/commit/630f1479c44f78484dfa21bb407cbe6f171dac87 https://github.com/openclaw/openclaw/commit/a47722de7e3c9cbda8d5512747ca7e3bb8f6ee66 https://github.com/openclaw/openclaw/security/advisories/GHSA-8883-9w57-vwv6 https://www.vulncheck.com/advisories/openclaw-unauthorized-action-execution-via-callback-dispatch
https://nvd.nist.gov/vuln/detail/CVE-2026-6012	8,8	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	D-Link DIR-513 1.10	https://lavender-bicycle-a5a.notion.site/D-Link-DIR-513-formSetPassword-33153a41781f806e9a3cf63a5a9091ac?source=copy_link https://vuldb.com/submit/791858 https://vuldb.com/vuln/356568 https://vuldb.com/vuln/356568/cti https://www.dlink.com/

https://nvd.nist.gov/vuln/detail/CVE-2026-6013	**8,8**	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	D-Link DIR-513 1.1	https://lavender-bicycle-a5a.notion.site/D-Link-DIR-513-formSetRoute-33153a41781f80f7aed1d3614c199d85?source=copy_link https://vuldb.com/submit/791859 https://vuldb.com/vuln/356569 https://vuldb.com/vuln/356569/cti https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-6014	**8,8**	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	D-Link DIR-513 1.10	https://lavender-bicycle-a5a.notion.site/D-Link-DIR-513-formAdvanceSetup-33153a41781f80829d47ec9b86dd8abf?source=copy_link https://vuldb.com/submit/791860 https://vuldb.com/vuln/356570 https://vuldb.com/vuln/356570/cti https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-6015	**8,8**	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda AC9 15.03.02.13	https://lavender-bicycle-a5a.notion.site/Tenda-AC9-QuickIndex-33153a41781f80458940f212f150a4fb?source=copy_link https://vuldb.com/submit/791828 https://vuldb.com/vuln/356571 https://vuldb.com/vuln/356571/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-6016	**8,8**	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda AC9 15.03.02.13	https://lavender-bicycle-a5a.notion.site/Tenda-AC9-WizardHandle-33153a41781f808480f9e3b78ce438e0?source=copy_link https://vuldb.com/submit/791829 https://vuldb.com/vuln/356572 https://vuldb.com/vuln/356572/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-6124	**8,8**	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda F451 1.0.0.7	https://github.com/Jimi-Lab/cve/issues/16 https://vuldb.com/submit/792874 https://vuldb.com/vuln/356987 https://vuldb.com/vuln/356987/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-6137	**8,8**	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda F451 1.0.0.7_cn_svn7958	https://github.com/Jimi-Lab/cve/issues/22 https://vuldb.com/submit/792881 https://vuldb.com/vuln/357001 https://vuldb.com/vuln/357001/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-6157	**8,8**	Totolink	Improper Restriction of Operations within the Bounds of a Memory Buffer	Totolink A800R 4.1.2cu.5137_B20200730	https://github.com/xyh4ck/iot_poc/blob/main/TOTOLINK/A800R/01_Buffer_Overflow_setAppEasyWizardConfig.md https://vuldb.com/submit/793114 https://vuldb.com/vuln/357037 https://vuldb.com/vuln/357037/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-6168	**8,8**	Totolink	Improper Restriction of Operations within the Bounds of a Memory Buffer	TOTOLINK A7000R up to 9.1.0u.6115	https://github.com/zhuchan770/vulnerability/blob/main/A7000R/setWiFiEasy-GuestCfg/ToToLink%20A7000R%20setWiFiEasy-GuestCfg%20338996b67c9780b89829d0ea70058788.md https://vuldb.com/submit/797193 https://vuldb.com/vuln/357056

					https://vuldb.com/vuln/357056/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-6186	**8,8**	UTT	Improper Restriction of Operations within the Bounds of a Memory Buffer	UTT HiPER 1200GW up to 2.5.3-170306	https://github.com/lin-3-start/lin-cve/blob/main/Amao/1.md https://vuldb.com/submit/797304 https://vuldb.com/vuln/357108 https://vuldb.com/vuln/357108/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-6194	**8,8**	Totolink	Improper Restriction of Operations within the Bounds of a Memory Buffer	Totolink A3002MU B20211125.1046	https://github.com/zhuchan770/vulnerability/blob/main/A3002MU/formWlanSetup/ToToLinkA3002MU%20formWlanSetup%20339996b67c9780caafb2d351dfd8a889.md https://vuldb.com/submit/797452 https://vuldb.com/vuln/357116 https://vuldb.com/vuln/357116/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-6199	**8,8**	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda F456 1.0.0.5	https://github.com/Litengzheng/vuldb_new/blob/main/F456/vul_116/README.md VulDB https://vuldb.com/submit/797471 VulDB https://vuldb.com/vuln/357121 VulDB https://vuldb.com/vuln/357121/cti VulDB https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-6200	**8,8**	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda F456 1.0.0.5	https://github.com/Litengzheng/vuldb_new/blob/main/F456/vul_117/README.md https://vuldb.com/submit/797472 https://vuldb.com/vuln/357122 https://vuldb.com/vuln/357122/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-5483	**8,5**	Red Hat	Insertion of Sensitive Information Into Sent Data	A flaw was found in odh-dashboard in Red Hat Openshift AI	https://access.redhat.com/errata/RHSA-2026:7397 https://access.redhat.com/errata/RHSA-2026:7398 https://access.redhat.com/errata/RHSA-2026:7403 https://access.redhat.com/errata/RHSA-2026:7404 https://access.redhat.com/security/cve/CVE-2026-5483 https://bugzilla.redhat.com/show_bug.cgi?id=2454764
https://nvd.nist.gov/vuln/detail/CVE-2019-25689	**8,4**	HTML5 Video Player	Out-of-bounds Write	HTML5 Video Player 1.2.5	http://www.html5videoplayer.net/download.html https://www.exploit-db.com/exploits/46279 https://www.vulncheck.com/advisories/html5-video-player-local-buffer-overflow-non-seh
https://nvd.nist.gov/vuln/detail/CVE-2026-35670	**8,1**	OpenClaw	Reliance on Untrusted Inputs in a Security Decision	OpenClaw before 2026.3.22	https://github.com/openclaw/openclaw/commit/630f1479c44f78484dfa21bb407cbe6f171dac87 https://github.com/openclaw/openclaw/commit/7ade3553b74ee3f461c4acd216653d5ba411f455 https://github.com/openclaw/openclaw/security/advisories/GHSA-wv46-v6xc-2qhf https://www.vulncheck.com/advisories/openclaw-webhook-reply-rebinding-via-username-resolution-in-synology-chat
https://nvd.nist.gov/vuln/detail/CVE-2026-40188	**7,7**	goshs is a SimpleHTTPServer written in Go	Missing Write Protection for Parametric Data Values	From 1.0.7 to before 2.0.0-beta.4	https://github.com/patrickhener/goshs/commit/141c188ce270ffbec087844a50e5e695b7da7744 https://github.com/patrickhener/goshs/releases/tag/v2.0.0-beta.4 https://github.com/patrickhener/goshs/security/advisories/GHSA-2943-crp8-38xx

https://nvd.nist.gov/vuln/detail/CVE-2026-33710	**7,5**	Chamilo LMS	Use of Insufficiently Random Values	Prior to 1.11.38 and 2.0.0-RC.3	https://github.com/chamilo/chamilo-lms/commit/4448701bb8ec557e94ef02d19c72cbe9c49c2d09 https://github.com/chamilo/chamilo-lms/commit/e7400dd840586ae134b286d0a2374f3d269a9a9d https://github.com/chamilo/chamilo-lms/security/advisories/GHSA-rpmg-j327-mr39
https://nvd.nist.gov/vuln/detail/CVE-2026-6024	**7,3**	Tenda	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Tenda i6 1.0.0.7(2204)	https://github.com/Litengzheng/vuldb_new/blob/main/M3/vul_84/README.md https://vuldb.com/submit/791826 https://vuldb.com/vuln/356600 https://vuldb.com/vuln/356600/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-6158	**7,3**	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink N300RH 6.1c.1353_B20190305	https://github.com/xyh4ck/iot_poc/tree/main/TOTOLINK/N300RHv4/02_setUpgradeUboot_RCE https://vuldb.com/submit/796426 https://vuldb.com/vuln/357038 https://vuldb.com/vuln/357038/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-40436	**7,1**	ZTE		ZTE ZXEDM iEMS	https://support.zte.com.cn/zte-iccp-isupport-webui/support/bulletin/security?lang=en_US&t=0.7465962531829456

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 Seven Known Exploited Vulnerabilities to Catalog	▪ CVE-2012-1854 Microsoft Visual Basic for Applications Insecure Library Loading Vulnerability ▪ CVE-2020-9715 Adobe Acrobat Use-After-Free Vulnerability ▪ CVE-2023-21529 Microsoft Exchange Server Deserialization of Untrusted Data Vulnerability ▪ CVE-2023-36424 Microsoft Windows Out-of-Bounds Read Vulnerability ▪ CVE-2025-60710 Microsoft Windows Link Following Vulnerability ▪ CVE-2026-21643 Fortinet SQL Injection Vulnerability ▪ CVE-2026-34621 Adobe Acrobat and Reader Prototype Pollution Vulnerability	https://www.cisa.gov/news-events/alerts/2026/04/13/cisa-adds-seven-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
Rockstar's GTA Game Hacked – Attackers published 78.6 Million Records Online	https://cybersecuritynews.com/rockstars-gta-game-hacked/
Claude AI Reportedly Down for Hundreds of Users With Intermittent 500 Errors	https://cybersecuritynews.com/claude-ai-reportedly-down/
Mozilla Criticizes Microsoft for Installing Copilot on Windows Without User Consent	https://cybersecuritynews.com/mozilla-criticizes-microsoft-for-copilot/
How Threat Intelligence Drives a Real ROI Boost for Your SOC	https://cybersecuritynews.com/how-threat-intelligence-drives-a-real-roi-boost-for-your-soc/
Nginx 1.29.8 and FreeNginx Released With Critical Security Updates	https://cybersecuritynews.com/nginx-1-29-8-and-freenginx-released/
Microsoft Confirms Recent Windows 11 Updates Break Push Button Reset	https://cybersecuritynews.com/windows-11-updates-break-push-button-reset/
WhatsApp's 'End-to-End Encryption by Default' Claim Called Major Consumer Fraud by Pavel Durov	https://cybersecuritynews.com/whatsapp-end-to-end-encryption-pavel-durov/
OpenAI Warns macOS Users to Update ChatGPT and Codex Immediately	https://cybersecuritynews.com/openai-macos-users/
Google Launches Gmail End-to-End Encryption for Android and iOS Users	https://cybersecuritynews.com/gmail-end-to-end-encryption-for-android-and-ios/
Google Unveils Device-Bound Chrome Sessions in Anti-Cookie-Theft Move	https://cybersecuritynews.com/device-bound-chrome-sessions-in-anti-cookie-theft-move/
Ransomware Gangs Expand Use of EDR Killers Beyond Vulnerable Drivers, ESET Warns	https://cybersecuritynews.com/ransomware-gangs-expand-use-of-edr-killers/
Hacker Uses Claude and ChatGPT to Breach Multiple Government Agencies	https://cybersecuritynews.com/hacker-uses-claude-and-chatgpt-to-breach/
Anthropic Launches Claude Beta for Word, Bringing AI-Powered Editing to Microsoft Docs	https://cybersecuritynews.com/claude-beta-for-word/
AI Router Vulnerabilities Allow Attackers to Inject Malicious Code and Steal Sensitive Data	https://cybersecuritynews.com/ai-router-vulnerabilities/
CPUID Website Compromised to Deliver Weaponized HWMonitor and CPU-Z Tools	https://cybersecuritynews.com/cpuid-website-compromised/
Hackers Use SVG Onload Trick to Hide Magecart Skimmer on Magento Checkout Pages	https://cybersecuritynews.com/svg-onload-trick-magecart-skimmer/
Single Line of Code Can Jailbreak 11 AI models Including ChatGPT, Claude, and Gemini	https://cybersecuritynews.com/single-line-of-code-can-jailbreak-11-ai-models/
WhatsApp Introduces Username Feature for Connecting Without Sharing Phone Numbers	https://cybersecuritynews.com/whatsapp-username-feature/

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
Basic-Fit Data Breach Exposes Millions of Users Across Multiple Countries	https://cybersecuritynews.com/basic-fit-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
Marimo RCE Vulnerability Exploited in the Within 10 Hours of Disclosure	https://cybersecuritynews.com/marimo-rce-vulnerability-exploited/
Critical Axios Vulnerability Allows Remote Code Execution – PoC Released	https://cybersecuritynews.com/axios-vulnerability-poc-released/
Apache Tomcat Vulnerabilities Enables Bypass of EncryptInterceptor	https://cybersecuritynews.com/apache-tomcat-vulnerabilities-encryptinterceptor/
Adobe Patches Acrobat Reader 0-Day Vulnerability Exploited in the Wild	https://cybersecuritynews.com/adobe-0-day-vulnerability-exploited/
Hackers Exploit GitHub Copilot Vulnerability to Exfiltrate Sensitive Data	https://cybersecuritynews.com/hackers-exploit-github-copilot-flaw/
HPE Aruba Private 5G Platform Vulnerability Enables Credential Theft Attacks	https://cybersecuritynews.com/hpe-aruba-private-5g-platform-vulnerability/
Multiple TP-Link Vulnerabilities Allow Attackers to Seize Control of the Device	https://cybersecuritynews.com/multiple-tp-link-vulnerabilities-seize-control-of-the-device/
Juniper Networks Default Password Vulnerability Let Attacker Take Full Control of the Device	https://cybersecuritynews.com/juniper-networks-default-password-vulnerability/
React Server Components Vulnerability Enables DoS Attacks	https://cybersecuritynews.com/react-server-components-vulnerability-2/
AWS Patches Critical RCE and Privilege Escalation Vulnerability in RES	https://cybersecuritynews.com/aws-patches/

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. Περι-λαμβάνονται αναφορές σε εργαλεία που χρησιμοποιούν οι επιτιθέμενοι, αλλά και δείκτες (IoCs) που μπορούν να χρησιμοποιηθούν στην άμυνα.

Σύντομη περιγραφή / Τίτλος	URL
Hackers Use Fake Proxifier Installer on GitHub to Spread ClipBanker Crypto-Stealing Malware	https://cybersecuritynews.com/hackers-use-fake-proxifier-installer-on-github/
Hackers Abuse GitHub and Jira Notifications to Deliver Phishing Through Trusted SaaS Channels	https://cybersecuritynews.com/hackers-abuse-github-and-jira-notifications/
Hackers Abuse MSBuild LOLBin to Evade Detection and Launch Fileless Windows At-tacks	https://cybersecuritynews.com/hackers-abuse-msbuild-lolbin/
Iran-Linked CyberAv3ngers Sets Sights on Water Utilities and Industrial Controllers	https://cybersecuritynews.com/iran-linked-cyberav3ngers-sets-sights/
Hackers Hide VIPERTUNNEL Python Backdoor Inside Fake DLL and Obfuscated Loader Chain	https://cybersecuritynews.com/hackers-hide-vipertunnel-python-backdoor/
APT37 Abuses Facebook, Telegram, and Tampered Installer in New Targeted Intru-sion Attack	https://cybersecuritynews.com/apt37-abuses-facebook-telegram/
Critical WordPress Plugin Flaw Lets Attackers Bypass Authentication and Gain Admin Access	https://cybersecuritynews.com/wordpress-plugin-flaw-lets-attackers-bypass-authentication/
Hackers Use AiTM Session Hijacking to Redirect Employee Salaries in New Storm-2755 Campaign	https://cybersecuritynews.com/hackers-use-aitm-session-hijacking/
Hackers Use Fake BTS World Tour Ticket Sites to Scam Fans Across Multiple Coun-tries	https://cybersecuritynews.com/hackers-use-fake-bts-world-tour-ticket-sites/
Censys Warns 5,219 Rockwell/Allen-Bradley PLCs Are Exposed Amid Iranian APT Ac-tivity	https://cybersecuritynews.com/censys-warns-5219-rockwell-allen-bradley-plcs/
Hackers Impersonate Secure Messaging Apps to Deploy ProSpy in Middle East Espio-nage Attacks	https://cybersecuritynews.com/hackers-impersonate-secure-messaging-apps-to-deploy-prospy/
Hackers Abuse GitHub and GitLab to Host Malware and Credential Phishing Cam-paigns	https://cybersecuritynews.com/hackers-abuse-github-and-gitlab/
MuddyWater Turns to Russian Malware-as-a-Service in New ChainShell Campaign	https://cybersecuritynews.com/muddywater-turns-to-russian-malware-as-a-service/
Trojanized OpenVSX Extension Spreads GlassWorm Across VS Code, Cursor, and Windsurf	https://cybersecuritynews.com/trojanized-openvsx-extension-spreads-glassworm/
DesckVB RAT Uses Obfuscated JavaScript and Fileless .NET Loader to Evade Detec-tion	https://cybersecuritynews.com/desckvb-rat-uses-obfuscated-javascript/

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

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/