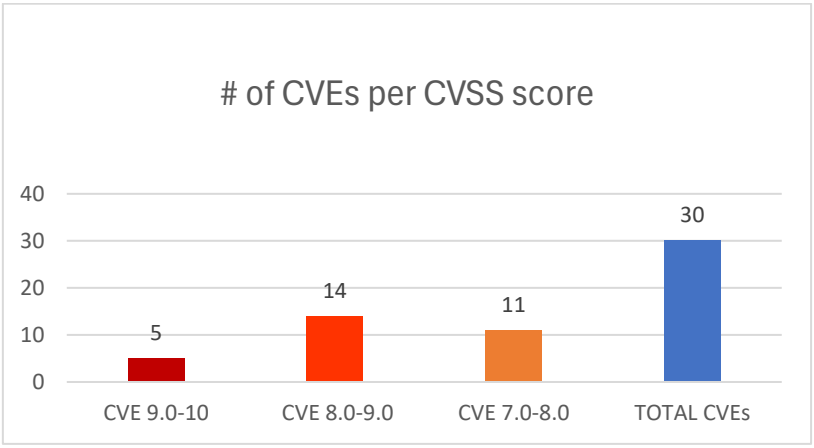
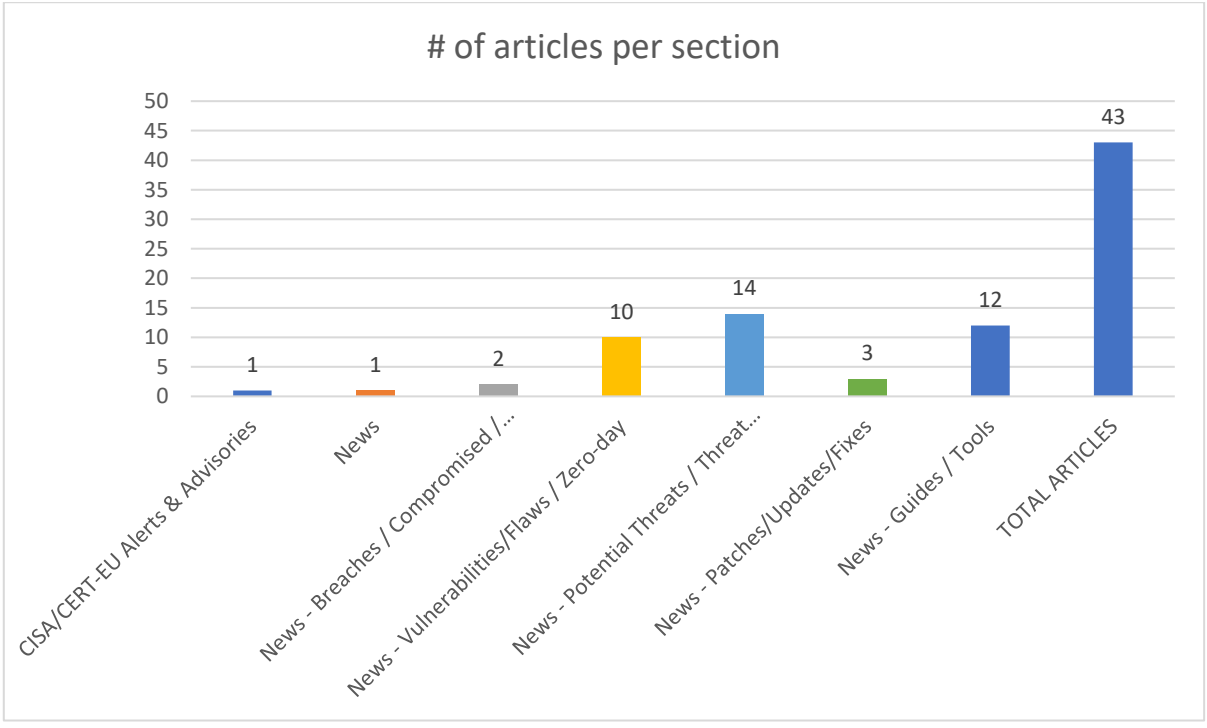
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 23/05/2026 - 26/05/2026





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://app.opencve.io/cve/CVE-2026-9384	9,3	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_331/README.md https://vuldb.com/submit/813429 https://vuldb.com/vuln/365347 https://vuldb.com/vuln/365347/cti https://www.totolink.net/
https://app.opencve.io/cve/CVE-2026-9408	9,3	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	A vulnerability was detected in Totolink A8000RU 7.1cu.643_b20200521	https://github.com/Litengzheng/vuldb_new2/blob/main/A8000RU/vul_340/README.md https://vuldb.com/submit/813443 https://vuldb.com/vuln/365389 https://vuldb.com/vuln/365389/cti https://www.totolink.net/
https://app.opencve.io/cve/CVE-2026-9433	9,3	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	A weakness has been identified in Totolink A8000RU 7.1cu.643_b20200521	https://github.com/Litengzheng/vuldb_new2/blob/main/A8000RU/vul_354/README.md https://vuldb.com/submit/813906 https://vuldb.com/vuln/365414 https://vuldb.com/vuln/365414/cti https://www.totolink.net/
https://app.opencve.io/cve/CVE-2026-9435	9,3	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	A vulnerability was detected in Totolink A8000RU 7.1cu.643_b20200521	https://github.com/Litengzheng/vuldb_new2/blob/main/A8000RU/vul_356/README.md https://vuldb.com/submit/813908 https://vuldb.com/vuln/365416 https://vuldb.com/vuln/365416/cti https://www.totolink.net/
https://app.opencve.io/cve/CVE-2026-9543	9,3	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	A vulnerability has been found in Totolink N300RH 6.1c.1353_B20190305	https://github.com/A1ester/TOTOLINK-N300RH-Command-Injection https://vuldb.com/submit/815068 https://vuldb.com/vuln/365607 https://vuldb.com/vuln/365607/cti https://www.totolink.net/

https://app.opencve.io/cve/CVE-2018-25358	8,7	D-Link	Exposure of Sensitive System Information to an Unauthorized Control Sphere	D-Link DIR601 2.02NA	http://ca.dlink.com/ http://support.dlink.ca/ProductInfo.aspx?m=DIR-601 https://www.exploit-db.com/exploits/45002 https://www.packetlabs.net https://www.vulncheck.com/advisories/d-link-dir601-2-02na-credential-disclosure-via-my-cgi-cgi
https://app.opencve.io/cve/CVE-2018-25368	8,7	Nord VPN	Memory Allocation with Excessive Size Value	Nord VPN 6.14.31	https://nordvpn.com/download/ VulnCheck https://www.vulncheck.com/advisories/nord-vpn-denial-of-service-via-password-field
https://app.opencve.io/cve/CVE-2026-44669	8,7	FACTION	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Prior to 1.8.3	https://github.com/factionsecurity/faction/releases/tag/1.8.3 https://github.com/factionsecurity/faction/security/advisories/GHSA-f2jc-wx44-mr54
https://app.opencve.io/cve/CVE-2026-9344	8,7	Edimax EW-7438RPn	Improper Restriction of Operations within the Bounds of a Memory Buffer	A security vulnerability has been detected in Edimax EW-7438RPn up to 1.31	https://github.com/wudipjq/my_vuln/blob/main/Edimax/vuln_2/2.md https://vuldb.com/submit/813885 https://vuldb.com/vuln/365307 https://vuldb.com/vuln/365307/cti
https://app.opencve.io/cve/CVE-2026-9429	8,7	Tenda F1202	Improper Restriction of Operations within the Bounds of a Memory Buffer	A vulnerability was found in Tenda F1202 1.2.0.20(408)	https://github.com/Litengzheng/vuldb_new2/blob/main/F1202/vul_31/README.md https://vuldb.com/submit/813912 https://vuldb.com/vuln/365410 https://vuldb.com/vuln/365410/cti https://www.tenda.com.cn/
https://app.opencve.io/cve/CVE-2026-9430	8,7	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda F1202 1.2.0.20(408)	https://github.com/Litengzheng/vuldb_new2/blob/main/F1202/vul_32/README.md https://vuldb.com/submit/813915 https://vuldb.com/vuln/365411 https://vuldb.com/vuln/365411/cti https://www.tenda.com.cn/
https://app.opencve.io/cve/CVE-2026-9632	8,7	UTT HiPER 1250GW	mproper Restriction of Operations within the Bounds of a Memory Buffer	A flaw has been found in UTT HiPER 1250GW up to 3.2.7-210907-180535.	https://github.com/luozhibo-sec/cve/blob/main/12.md https://vuldb.com/submit/818383 https://vuldb.com/vuln/365741 https://vuldb.com/vuln/365741/cti
https://app.opencve.io/cve/CVE-2026-42013	8,2	Red Hat	Improper Validation of Specified Quantity in Input	-	https://access.redhat.com/errata/RHSA-2026:20611 https://access.redhat.com/security/cve/CVE-2026-42013 https://bugzilla.redhat.com/show_bug.cgi?id=2467448
https://app.opencve.io/cve/CVE-2026-44728	8,2	Babel	Improper Control of Generation of Code ('Code Injection')	From 7.12.0 to before 7.29.4 and 8.0.0-alpha.13	https://github.com/babel/babel/security/advisories/GHSA-fv7c-fp4j-7gwp

https://app.opencve.io/cve/CVE-2026-48898	8,2	Joomla! Project	Insufficient Information	-	https://developer.joomla.org/security-centre/1045-20260513-core-privilege-escalation-through-com-users-batch-task.html
https://app.opencve.io/cve/CVE-2026-45361	8,1	Apache Airflow	Key Exchange without Entity Authentication	Users are advised to upgrade to `apache-airflow-providers-google` 22.0.0 or later.	http://www.openwall.com/lists/oss-security/2026/05/24/9 https://github.com/apache/airflow/pull/66746 https://lists.apache.org/thread/3lpj7ppwxp7jtp81rnxk75xvln7qd7h2
https://app.opencve.io/cve/CVE-2026-48131	8,1	Checkpoint Quantum Security Gateway	Heap-based Buffer Overflow	-	https://support.checkpoint.com/results/sk/sk184981
https://app.opencve.io/cve/CVE-2026-8855	8,1	IBM HTTP Server	Improper Control of Generation of Code ('Code Injection')	IBM HTTP Server 8.5 and 9.0	https://www.ibm.com/support/pages/node/7274065
https://app.opencve.io/cve/CVE-2026-8834	8,0	IBM HTTP Server	Heap-based Buffer Overflow	IBM HTTP Server 8.5, and 9.0	https://www.ibm.com/support/pages/node/7274065
https://app.opencve.io/cve/CVE-2025-43306	7,8	Apple macOS	Improper Privilege Management	A logic issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. A malicious app may be able to gain root privileges.	https://support.apple.com/en-us/125110 https://support.apple.com/en-us/125111 https://support.apple.com/en-us/125112
https://app.opencve.io/cve/CVE-2026-24192	7,8	NVIDIA	Incorrect Conversion between Numeric Types	-	https://nvd.nist.gov/vuln/detail/CVE-2026-24192 https://nvidia.custhelp.com/app/answers/detail/a_id/5821 https://www.cve.org/CVERecord?id=CVE-2026-24192
https://app.opencve.io/cve/CVE-2026-24193	7,8	NVIDIA	Out-of-bounds Write	-	https://nvd.nist.gov/vuln/detail/CVE-2026-24193 https://nvidia.custhelp.com/app/answers/detail/a_id/5821 https://www.cve.org/CVERecord?id=CVE-2026-24193
https://app.opencve.io/cve/CVE-2026-24194	7,8	NVIDIA	Improper Preservation of Permissions	-	https://nvd.nist.gov/vuln/detail/CVE-2026-24194 https://nvidia.custhelp.com/app/answers/detail/a_id/5821 https://www.cve.org/CVERecord?id=CVE-2026-24194
https://app.opencve.io/cve/CVE-2026-7454	7,8	Autodesk 3ds Max	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	-	https://www.autodesk.com/products/autodesk-access/overview https://www.autodesk.com/trust/security-advisories/adsk-sa-2026-0006

https://app.opencve.io/cve/CVE-2026-2253	**7,7**	Hitachi Vantara Pentaho Data Integration and Analytics	Improper Restriction of XML External Entity Reference	Hitachi Vantara Pentaho Data Integration & Analytics versions before 10.2.0.7 and 11.0.0.0, including 9.3.x and 8.3.x, does not prevent certain XML parsers from resolving external entities.	https://support.pentaho.com/hc/en-us/articles/45677548193933--Resolved-Hitachi-Vantara-Pentaho-Data-Integration-Analytics-Improper-Restriction-of-XML-External-Entity-Reference-Versions-before-10-2-0-7-and-11-0-0-0-Impacted-CVE-2026-2253
https://app.opencve.io/cve/CVE-2026-48829	**7,5**	GNU SASL	NULL Pointer Dereference	In GNU SASL before 2.2.3	https://codeberg.org/gsasl/gsasl/commit/da9b5ae2962b014879e4a406c3b38f25aa70e97a https://lists.debian.org/debian-security-announce/2026/msg00182.html https://lists.gnu.org/archive/html/help-gsasl/2026-05/msg00000.html https://lists.gnu.org/archive/html/help-gsasl/2026-05/msg00002.html
https://app.opencve.io/cve/CVE-2026-8850	**7,5**	IBM HTTP Server	NULL Pointer Dereference	IBM HTTP Server 8.5 and 9.0	https://www.ibm.com/support/pages/node/7274065
https://app.opencve.io/cve/CVE-2026-44730	**7,2**	OpenCTI-Platform	Improper Access Control	Prior to 6.9.7	https://github.com/OpenCTI-Platform/opencti/security/advisories/GHSA-q537-qhj4-wcjx
https://app.opencve.io/cve/CVE-2025-46284	**7,0**	Apple macOS	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	A race condition was addressed with additional validation. This issue is fixed in macOS Sequoia 15.7, macOS Tahoe 26. An app may be able to gain root privileges.	https://support.apple.com/en-us/125110 https://support.apple.com/en-us/125111
https://app.opencve.io/cve/CVE-2026-43503	**7,0**	Linux	-	-	https://git.kernel.org/stable/c/12401fcfb01f53ccc63ab0a3246570fe8f3105ee https://git.kernel.org/stable/c/179f1852bdedc300e373e807cc102cd81feff196 https://git.kernel.org/stable/c/48f6a5356a33dd78e7144ae1faef95ffc990aae0

					https://git.kernel.org/stable/c/989214c66884d70716d83dc1d0bf5e16287bf349 https://git.kernel.org/stable/c/9bc9d6d6967a2239aa57af2aa53554eddd640d20 https://git.kernel.org/stable/c/fbeab9555564a1b98e8582cd106dfe46c4606991 https://git.kernel.org/stable/c/fc6eb39c55e97df2f94ad974b8a5bbcd019da2c8 https://git.kernel.org/stable/c/ff375cc75f9167168db38e0464a482d5fbc8d81d

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-2026-48172 LiteSpeed cPanel Plugin Privilege Escalation Vulnerability**	**https://www.cisa.gov/news-events/alerts/2026/05/26/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
India’s CERT-In Asks Organizations to Patch Vulnerabilities in Systems Within 12 hours	https://cybersecuritynews.com/cert-in-asks-patch-vulnerabilities-12-hours/

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
Hackers Compromised 233 Versions of Laravel-Lang Packages by Hacking 700 GitHub Repos	https://cybersecuritynews.com/laravel-lang-packages-compromised/
Hackers Compromised 34 Packages in npm, PyPI, and Crates in New Supply Chain Attack	https://cybersecuritynews.com/supply-chain-trapdoor-malware/

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 7-Zip Vulnerabilities Let Attackers Execute Arbitrary Code and Compromise Systems	https://cybersecuritynews.com/7-zip-vulnerabilities-code-execution/
KnowledgeDeliver LMS Zero-Day Exploited to Deploy BLUEBEAM Web Shell	https://cybersecuritynews.com/knowledgedeliver-lms-zero-day-exploited/
CISA Warns of Drupal Core SQL Injection Vulnerability Exploited in Attacks	https://cybersecuritynews.com/drupal-core-sql-injection-vulnerability-exploited/
Nginx-poolslip Vulnerability Enables DoS and Code Execution Attacks — Patch Now!	https://cybersecuritynews.com/nginx-poolslip-vulnerability/
Ghost CMS SQL injection flaw exploited in large-scale ClickFix campaign	https://www.bleepingcomputer.com/news/security/ghost-cms-sql-injection-flaw-exploited-in-large-scale-clickfix-campaign/
Anthropic: Mythos Detected 23,000 Potential Vulnerabilities Across 1,000 OSS Projects	https://www.securityweek.com/anthropic-mythos-detected-23000-potential-vulnerabilities-across-1000-oss-projects/
LiteSpeed cPanel Plugin CVE-2026-48172 Exploited to Run Scripts as Root	https://thehackernews.com/2026/05/litespeed-cpanel-plugin-cve-2026-48172.html
BIND 9 Software Vulnerabilities Exposes Resolvers and Authoritative Servers to Remote Exploits	https://cybersecuritynews.com/bind-9-vulnerabilities-exposes/
Multiple Angular Language Service Extension Vulnerabilities Enable RCE Attacks	https://cybersecuritynews.com/angular-extension-vulnerabilities/
Microsoft SharePoint Server Vulnerability Enables Remote Code Execution Attacks	https://cybersecuritynews.com/sharepoint-server-rce-vulnerability/

Patches / Updates / Fixes

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

Σύντομη περιγραφή / Τίτλος	URL
Wireshark 4.6.6 Released With Fix for Dissector Crash via Malformed Packet Injection	https://cybersecuritynews.com/wireshark-4-6-6-released/
Anthropic Releases Free Security Plugin for Claude Code Terminal to Detect Vulnerabilities	https://cybersecuritynews.com/free-security-plugin-for-claude-code/
PuTTY 0.84 Released With Fix for SSH KEX Crashes and Telnet Prompt Spoofing Flaw	https://cybersecuritynews.com/putty-0-84-released/

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
InvisibleFerret Malware Now Ships as .pyd and .so Files to Evade Script Detection	https://cybersecuritynews.com/invisibleferret-malware-now-ships-as-pyd/
Cybercriminals Use Telegram Channels to Sell Verified Bank and Fintech Mule Accounts	https://cybersecuritynews.com/cybercriminals-use-telegram-channels/
Hackers Hide Linux Payload Under SSH-Like Filename During Package Installation	https://cybersecuritynews.com/hackers-hide-linux-payload-under-ssh-like-filename/
Russian Hacker Used Jailbroken Gemini to Steal Admin Credentials and Drain Crypto Wallets	https://cybersecuritynews.com/russian-hacker-used-jailbroken-gemini/
Hackers Abuse Shared CDN Infrastructure to Bypass Domain Reputation Security Controls	https://cybersecuritynews.com/hackers-abuse-shared-cdn-infrastructure/
Iranian APT Uses SEO Poisoning to Deliver Fake SQL Developer Malware Installer	https://cybersecuritynews.com/iranian-apt-uses-seo-poisoning/
Hackers Actives Scanning SonicWall Firewall Interfaces – 597,000 Sessions Observed	https://cybersecuritynews.com/hackers-scan-sonicwall-firewall-interfaces/
MiniUpdate RAT Uses Azure-Hosted C2 Domains for Targeted Espionage Campaigns	https://cybersecuritynews.com/miniupdate-rat-uses-azure-hosted-c2-domains/
Hackers Exploit F5 BIG-IP Appliance to Gain SSH Access and Pivot Into Enterprise Linux Networks	https://cybersecuritynews.com/f5-big-ip-exploited-for-ssh-access/
Hackers Use Browser-Locking CypherLoc Kit to Push Fake Microsoft Support Calls	https://cybersecuritynews.com/hackers-use-browser-locking-cypherloc-kit/
FBI Warns 'Kali365' Phishing Kit Hijacks Microsoft 365 OAuth Tokens	https://www.infosecurity-magazine.com/news/fbi-kali365-phishing-kit-m365/
Attackers Abuse Open RDP Ports to Gain Initial Access Into Business Networks	https://cybersecuritynews.com/attackers-abuse-open-rdp-ports/
New 0-Click WhatsApp Account Takeover Attack Targeting iOS 16 Users	https://cybersecuritynews.com/0-click-whatsapp-target-ios-16-users/
Quasar Linux RAT Targets Developers With Fileless Execution and eBPF Rootkit	https://cybersecuritynews.com/quasar-linux-rat-targets-developers/

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/

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/