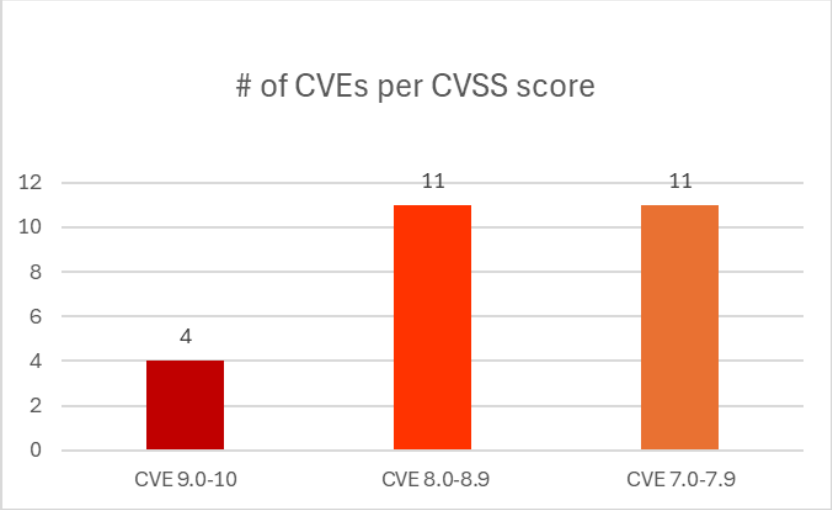
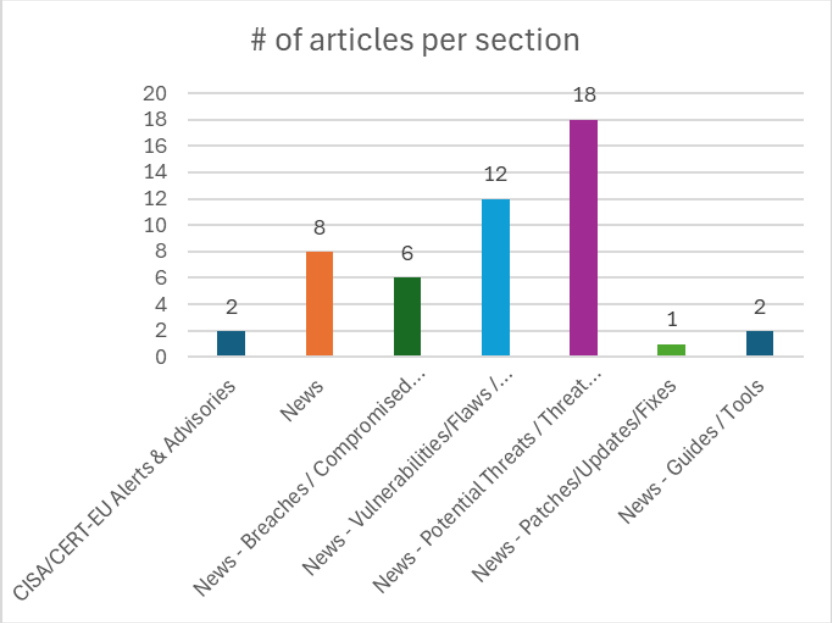
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 13/06/2026 - 16/06/2026





Contents

Common Vulnerabilities and Exposures (CVEs)

Η ενότητα αυτή εστιάζει σε ευπάθειες που έχουν καταχωρηθεί πρόσφατα και αξιολογούνται ως σοβαρές, με βάση τη βαθμολογία CVSS. Παρουσιάζονται με σαφήνεια τα συστήματα ή εφαρμογές που επηρεάζονται, ο τύπος της ευπάθειας (όπως SQL injection ή command injection) και σχετικοί σύνδεσμοι για περαιτέρω πληροφόρηση ή μέτρα αντιμετώπισης.

URL ευπάθειας (NIST NVD)	CVSSv 3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2026-12183	9,8	Nefteprodukttekhnika BUK TS-G Gas Station Automation System	Improper Authentication	2.9.1 through 2.10.2	https://bukts.ru/repo-bukts-current TuranSec https://cwe.mitre.org/data/definitions/287.html TuranSec https://cwe.mitre.org/data/definitions/306.html TuranSec https://github.com/ciprobe/bukts_auth_bypass
https://www.cve.org/CVERecord?id=CVE-2026-35273	9,8	Oracle PeopleSoft	Missing Authentication for Critical Function	PeopleSoft Enterprise PeopleTools, affected at 8.61, affected at 8.62	https://www.oracle.com/security-alerts/alert-cve-2026-35273.html
https://nvd.nist.gov/vuln/detail/CVE-2026-48886	9,3	S Help Desk	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	S Help Desk <= 3.0.9 versions	https://patchstack.com/database/wordpress/plugin/js-support-ticket/vulnerability/wordpress-js-help-desk-plugin-3-0-9-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-49952	9,1	Discuz!	Reusing a Nonce, Key Pair in Encryption	Discuz! X5.0 releases 20260320 through 20260501	https://gitee.com/Discuz/DiscuzX/commit/9962dad52c4c6999dabaf91ecd70377c680ff3c6 https://karmainsecurity.com/KIS-2026-09 https://karmainsecurity.com/chaining-bugs-in-discuz-from-race-condition-to-rce https://www.vulncheck.com/advisories/discuz-x5-0-authentication-bypass-via-dbbak-php-encryption-oracle
https://nvd.nist.gov/vuln/detail/CVE-2026-12174	8,8	D-Link DCS-935L	Improper Restriction of Operations within the Bounds of a Memory Buffer	1.10.01	https://github.com/Real-Simplicity/cve-database/tree/main/CVE_Report_DLink_DCS935L_Format_String
https://nvd.nist.gov/vuln/detail/CVE-2026-12186	8,8	GL.iNet GL-MT3000	Improper Neutralization of Special Elements used in a Command ('Command Injection')	up to 4.4.5	https://fw.gl-inet.com/firmware/mt3000/release/mt3000-4.8.1-0819-1755615825.tar VulDB https://github.com/StrTzz123/iot_vul/blob/main/GL-iNet/MT3000/4.4.5/tor_set_config/Readme.md
https://nvd.nist.gov/vuln/detail/CVE-2026-12187	8,8	GL.iNet	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	GL.iNet GL-MT3000 up to 4.4.5	https://fw.gl-inet.com/firmware/mt3000/release/mt3000-4.8.1-0819-1755615825.tar https://github.com/StrTzz123/iot_vul/tree/main/GL-iNet/MT3000/4.4.5/upgrade_online_url https://vuldb.com/cve/CVE-2026-12187 https://vuldb.com/submit/815654

					https://vuldb.com/vuln/370833 https://vuldb.com/vuln/370833/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-39478	8,8	Anti-Malware Security and Brute-Force Firewall	Deserialization of Untrusted Data	Anti-Malware Security and Brute-Force Firewall <= 4.23.87 versions	https://patchstack.com/database/wordpress/plugin/gotmls/vulnerability/wordpress-anti-malware-security-and-brute-force-firewall-plugin-4-23-87-php-object-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-7273	8,8	Zyxel	Stack-based Buffer Overflow	CGI program of Zyxel GS1900-48HPv2 firmware versions through 2.90(ABTQ.1)C0	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-stack-based-buffer-overflow-vulnerability-in-gs1900-series-switches-06-16-2026
https://nvd.nist.gov/vuln/detail/CVE-2026-47825	8,6	Spring Cloud Gateway Server	Origin Validation Error	Affected versions: Spring Cloud Gateway 3.1.x (fix 3.1.13). Spring Cloud Gateway 4.1.x (fix 4.1.13). Spring Cloud Gateway 4.2.x (fix 4.2.9). Spring Cloud Gateway 4.3.x (fix 4.3.5). Spring Cloud Gateway 5.0.x (fix 5.0.2).	https://spring.io/security/cve-2026-47825
https://nvd.nist.gov/vuln/detail/CVE-2026-47835	8,6	Spring AI Vector Stores	Improper Neutralization of Special Elements in Data Query Logic	Affected versions: Spring AI 1.0.0 through 1.0.x (fix 1.0.9). Spring AI 1.1.0 through 1.1.x (fix 1.1.8).	https://spring.io/security/cve-2026-47835
https://nvd.nist.gov/vuln/detail/CVE-2026-52697	8,5	Taskbuilder	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Taskbuilder <= 5.0.7 versions	https://patchstack.com/database/wordpress/plugin/taskbuilder/vulnerability/wordpress-taskbuilder-plugin-5-0-7-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-54420	8,5	LiteSpeed cPanel	UNIX Symbolic Link (Symlink) Following	LiteSpeed cPanel plugin before 2.4.8 (as distributed in LiteSpeed WHM PlugIn before 5.3.2.0)	https://blog.litespeedtech.com/2026/06/01/security-update-for-litespeed-cpanel-plugin-2/ https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-54420 https://www.litespeedtech.com/products/litespeed-web-server/control-panel-support/cpanel
https://nvd.nist.gov/vuln/detail/CVE-2026-54412	8,2	LiamBindle MQTT-C	Out-of-bounds Read	through version 1.1.6	https://cwe.mitre.org/data/definitions/125.html TuranSec https://cwe.mitre.org/data/definitions/191.html TuranSec https://github.com/LiamBindle/MQTT-C TuranSec https://github.com/LiamBindle/MQTT-C/blob/v1.1.6/src/mqtt.c#L1334
https://nvd.nist.gov/vuln/detail/CVE-2026-12222	8,0	Yealink	Improper Restriction of Operations within the Bounds of a Memory Buffer	Yealink SIP-T46U 108.86.0.118	http://cdn2.v50to.cc/T46U/T46U_mod_webd_BlueToothTest_off_by_one.zip https://vuldb.com/cve/CVE-2026-12222 https://vuldb.com/submit/834602 https://vuldb.com/vuln/370865 https://vuldb.com/vuln/370865/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-12191	7,8	Comma AI Openpilot	Improper Input Validation	0.11	https://vuldb.com/cve/CVE-2026-12191
https://nvd.nist.gov/vuln/detail/CVE-2026-12193	7,8	VS Revo	Improper Restriction of Operations within the	VS Revo RevoUninstaller 2.5.x/2.6.x	https://github.com/Kalagious/RevoDetectorExploit/tree/master https://jordanhiggins.blog/revouninstaller-pool-overflow-exploit/ https://vandalsuidaho-my.sharepoint.com/:w:/g/personal/higg2059_van-

			Bounds of a Memory Buffer		dals_uidaho_edu/IQAMHgdfpRAkSqDsoFVswIYNAXjPVFz-ad-mcJyl5ITzYhu0?e=4Ywwza https://vuldb.com/cve/CVE-2026-12193 https://vuldb.com/submit/829132 https://vuldb.com/submit/829133 https://vuldb.com/vuln/370839 https://vuldb.com/vuln/370839/cti https://www.revouninstaller.com/start-freeware-download/ https://youtu.be/JR0KPjWRTns?si=Ff2bUDvv3butJyfP
https://nvd.nist.gov/vuln/detail/CVE-2026-12214	7,8	Qihoo 360 Total Security		Protection Mechanism Failure	https://github.com/Gach0ng/vuldb_submit/issues/4 https://vuldb.com/cve/CVE-2026-12214 https://vuldb.com/submit/833135 https://vuldb.com/vuln/370858 https://vuldb.com/vuln/370858/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-12217	7,8	DVDFab Virtual Drive	Incorrect Privilege Assignment	DVDFab Virtual Drive 2.0.0.5	https://vuldb.com/cve/CVE-2026-12217 https://vuldb.com/submit/833857 https://vuldb.com/vuln/370860 https://vuldb.com/vuln/370860/cti https://winslow1984.com/books/cve-collection/page/dvdfab-virtual-drive-kernel-driver-dvdfabiosys-local-privilege-escalation
https://nvd.nist.gov/vuln/detail/CVE-2026-6428	7,6	reports/catalogue_out.pl in Koha Community	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	through 22.11.37, 23.x, 24.x before 24.11.16, 25.05.x before 25.05.11, 25.11.x before 25.11.05, 26.05.x before 26.05.01, and 26.11.x before 26.11.00	https://bugs.koha-community.org/bugzilla3/attachment.cgi?id=199539
https://nvd.nist.gov/vuln/detail/CVE-2026-52695	7,5	ABC Crypto Checkout	Insertion of Sensitive Information Into Sent Data	ABC Crypto Checkout <= 1.8.2 versions	https://patchstack.com/database/wordpress/plugin/payerurl-crypto-currency-payment-gateway-for-woocommerce/vulnerability/wordpress-abc-crypto-checkout-plugin-1-8-2-sensitive-data-exposure-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-12200	7,3	Ritlabs	Improper Restriction of Operations within the Bounds of a Memory Buffer	Ritlabs TinyWeb Server up to 1.94 on Win32	https://nathan2.com/posts/tinyweb/ https://vuldb.com/cve/CVE-2026-12200 https://vuldb.com/submit/829894 https://vuldb.com/vuln/370842 https://vuldb.com/vuln/370842/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-12204	7,3	ShopXO	Improper Authorization	ShopXO up to 6.7.1	https://github.com/yunyan05/MYCVE/tree/main/ShopXO/V6.7.1-Unauthenticated-Crontab-Trigger https://vuldb.com/cve/CVE-2026-12204 https://vuldb.com/submit/830800 https://vuldb.com/vuln/370847 https://vuldb.com/vuln/370847/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-12197	7,2	Ruijie	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	Ruijie EG105G-P 2.340	https://github.com/ictrun/java/issues/6 https://vuldb.com/cve/CVE-2026-12197 https://vuldb.com/submit/829253 https://vuldb.com/vuln/370840 https://vuldb.com/vuln/370840/cti

https://nvd.nist.gov/vuln/detail/CVE-2026-5513	**7,2**	The Online Scheduling and Appointment Booking System – Bookly plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 27.2	https://plugins.trac.wordpress.org/changeset/3504922/bookly-responsive-appointment-booking-tool Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/b8ab6dfa-3764-470f-aa49-1964f42d93de?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-9109	**7,2**	GPTranslate	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	The GPTranslate – Multilingual AI Translation for WordPress: Automatically Translate Websites plugin for WordPress is vulnerable to Stored Cross-Site Scripting via REST API Translation Storage in all versions up to, and including, 2.31	https://plugins.trac.wordpress.org/browser/gptranslate/tags/2.27.5/assets/js/admin.js#L1 https://plugins.trac.wordpress.org/browser/gptranslate/tags/2.27.5/gptranslate.php#L1134 https://plugins.trac.wordpress.org/browser/gptranslate/tags/2.27.5/gptranslate.php#L3578 https://plugins.trac.wordpress.org/browser/gptranslate/tags/2.27.5/gptranslate.php#L3654 https://plugins.trac.wordpress.org/browser/gptranslate/tags/2.31/assets/js/admin.js#L1 https://plugins.trac.wordpress.org/browser/gptranslate/tags/2.31/gptranslate.php#L1134 https://plugins.trac.wordpress.org/browser/gptranslate/tags/2.31/gptranslate.php#L3578 https://plugins.trac.wordpress.org/browser/gptranslate/tags/2.31/gptranslate.php#L3654 https://plugins.trac.wordpress.org/browser/gptranslate/tags/2.32/assets/js/admin.js#L1 https://plugins.trac.wordpress.org/browser/gptranslate/tags/2.32/gptranslate.php#L1104 https://plugins.trac.wordpress.org/browser/gptranslate/tags/2.32/gptranslate.php#L3574 https://www.wordfence.com/threat-intel/vulnerabilities/id/1c93b564-5428-4b0e-bbe8-f1e1e68940ac?source=cve

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-2026-35273 Oracle PeopleSoft Enterprise PeopleTools Missing Authentication for Critical Function Vulnerability	https://www.cisa.gov/news-events/alerts/2026/06/12/cisa-adds-one-known-exploited-vulnerability-catalog
CISA Adds Two Known Exploited Vulnerabilities to Catalog	▪ CVE-2026-20262 Cisco Catalyst SD-WAN Manager Directory or Path Traversal Vulnerability ▪ CVE-2026-54420 LiteSpeed cPanel Plugin UNIX Symbolic Link (Symlink) Following Vulnerability	https://www.cisa.gov/news-events/alerts/2026/06/15/cisa-adds-two-known-exploited-vulnerabilities-catalog

News

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

Σύντομη περιγραφή / Τίτλος	URL
Anthropic Updated Privacy Policy to Include Identity Verification for Claude Users	https://cybersecuritynews.com/anthropic-updated-privacy-policy/
Windows 11 Update KB5094126 Freezes Systems, Forces BitLocker Recovery, and More	https://cybersecuritynews.com/windows-11-update-kb5094126/
Threat Actor Malware Platform Exposed via Unlocked PHP Installation Page	https://cybersecuritynews.com/malware-platform-unlocked-php-installation-page/
BugHunter – Bug Bounty Toolkit Powered by Claude and Free AI Providers	https://cybersecuritynews.com/bughunter-bug-bounty-toolkit/
Facebook and Instagram Down Globally, Users Reporting Multiple Issues	https://cybersecuritynews.com/facebook-and-instagram-down-globally/
Google Sues Chinese Cybercrime Network for Using Gemini AI to Launch Cyberattacks	https://cybersecuritynews.com/google-sues-chinese-cybercrime-network/
Authorities Dismantle Cryptocurrency Laundering Services ‘AudiA6’ Used by Ransomware Gangs	https://cybersecuritynews.com/authorities-dismantle-audia6-services/
CISA Requires Federal Agencies to Patch Critical Vulnerabilities Within 3 Days	https://cybersecuritynews.com/cisa-patch-vulnerabilities-3-days/

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 Abuse Legitimate RMM Tools in The Quarry IRS and SSA Phishing Campaigns	https://cybersecuritynews.com/hackers-abuse-legitimate-rmm-tools/
SHADOWBYT3$ Allegedly Claim Breach of Nintendo, Stealing Sensitive Data	https://cybersecuritynews.com/shadowbyt3-claim-breach-of-nintendo/
Maine Takes Data Breach Reporting Portal Offline After Fake VRChat and Discord Filings	https://cybersecuritynews.com/maine-data-breach-portal-offline/
400+ Arch Linux AUR Packages Compromised in a Supply Chain Attack Deploying Infostealers	https://cybersecuritynews.com/arch-linux-aur-packages-compromised/
Critical Vulnerability Chain in LangGraph Allows Attackers to Gain Full Server Control	https://cybersecuritynews.com/vulnerability-chain-in-langgraph/
OceanLotus APT Compromises FireAnt MetaKit in Supply-Chain Attack on Stock Investors	https://cybersecuritynews.com/oceanlotus-apt-compromises-fireant-metakit/

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
LiteSpeed cPanel Plugin 0-Day Vulnerability Actively Exploited in the Wild	https://cybersecuritynews.com/litespeed-cpanel-plugin-0-day-vulnerability-exploit/
Cisco SD-WAN vManage Vulnerability Exploited in Zero-Day Attacks	https://cybersecuritynews.com/cisco-sd-wan-vmanage-vulnerability-exploit/
Microsoft Site Showing Warning Following Certificate Expiry	https://cybersecuritynews.com/microsoft-certificate-expiry/
Critical Microsoft 365 Copilot Vulnerability Allows Attackers to Steal Data in One Click	https://cybersecuritynews.com/microsoft-365-copilot-one-click-vulnerability/
Critical Wazuh Vulnerability Lets Attackers Tamper with Alerts and Delete Security Evidence	https://cybersecuritynews.com/wazuh-vulnerability/
WinRAR Vulnerability Exploited by Russian Hackers to Deploy GIFTEDCROOK Stealer	https://cybersecuritynews.com/winrar-vulnerability-exploited-by-russian-hackers/
Palo Alto Warns of GlobalProtect VPN Vulnerability Actively Exploited in the Wild	https://cybersecuritynews.com/palo-alto-vpn-vulnerability-exploited/
Splunk Enterprise Pre-Auth RCE Chain Exposes Database With Zero Authentication	https://cybersecuritynews.com/splunk-enterprise-pre-auth-rce-chain-exposes/
Microsoft Outlook and Word Vulnerabilities Allow Attackers to Execute Malicious Code	https://cybersecuritynews.com/microsoft-outlook-and-word-vulnerabilities/
Palo Alto PAN-OS Vulnerability Allows Attackers to Execute Arbitrary Commands as Root User	https://cybersecuritynews.com/palo-alto-pan-os-vulnerability/

Microsoft Teams for Android Vulnerability Allows Attackers to Disclose Sensitive Data	https://cybersecuritynews.com/microsoft-teams-for-android-vulnerability/
Oracle PeopleSoft 0-Day RCE Vulnerability Exploited in Attacks by ShinyHunters	https://cybersecuritynews.com/oracle-peoplesoft-0-day-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
Google Patches 28 Chrome Vulnerabilities that Allow Attackers to Execute Malicious Code	https://cybersecuritynews.com/28-chrome-vulnerabilities-patched/

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
OptinMonster Plugin Hack Exposes 1.2 Million WordPress Sites to Cyberattack	https://cybersecuritynews.com/optinmonster-plugin-exposes-wordpress-sites/
Ransomware Ecosystem Consolidates Around LockBit Alumni, Qilin, Hyflock, and The Gentlemen	https://cybersecuritynews.com/ransomware-ecosystem-consolidates/
Nearly 14,000 SimpleHelp Servers Exposed Amid Critical Authentication Bypass Disclosure	https://cybersecuritynews.com/simplehelp-servers-exposed-authentication-bypass-disclosure/
Hackers Use Microsoft Graph Reconnaissance to Target Payroll and HR Employees	https://cybersecuritynews.com/hackers-use-microsoft-graph-reconnaissance/
China-Nexus Hackers Use Backdoored PAM Modules for Credential Theft and Authentication Bypass	https://cybersecuritynews.com/china-nexus-hackers-use-backdoored-pam-modules/
SearchJack Campaign Uses 23 Chrome Extensions to Hijack Searches of 758,000 Users	https://cybersecuritynews.com/searchjack-campaign-uses-23-chrome-extensions/
PromptSnatcher Ad Blocker Extensions Steal AI Chats From ChatGPT, Claude, and Gemini	https://cybersecuritynews.com/promptsnatcher-ad-blocker-extensions-steal-ai-chats/
Hackers Abuse LNK Files, PowerShell, and Python Loader to Deploy NarwhalRAT	https://cybersecuritynews.com/powershell-and-python-loader-to-deploy-narwhalrat/
152 Chrome Extensions Hide Ad Tracking and Fake Google Search Traffic	https://cybersecuritynews.com/chrome-extensions-hide-ad-tracking/
New Agentjacking Attack Hijacks Your AI Coding Agent to Run Code From a Hacker's Server	https://cybersecuritynews.com/agentjacking-attack-hijacks-ai-coding-agent/
Fancy Bear Hackers Abuse EdgeRouters and Cloud Services to Launch Stealthy Cyberattacks	https://cybersecuritynews.com/fancy-bear-hackers-abuse-edgerouters-and-cloud-services/

Hackers Abuse Legitimate NinjaOne RMM Software to Bypass Traditional Malware Detection	https://cybersecuritynews.com/hackers-abuse-legitimate-ninjaone-rmm-software/
Malicious npm Campaign Steals SSH Keys, API Tokens, Cloud Credentials, and Wallet Secrets	https://cybersecuritynews.com/malicious-npm-campaign-steals-ssh-keys-api-tokens/
Hackers Use OnyxC2 Malware-as-a-Service to Steal Credentials From 210 Applications	https://cybersecuritynews.com/hackers-use-onyxc2-malware-as-a-service/
SHEETCREEP C# RAT Abuses Google Sheets API as C2 to Target Diplomatic Organizations	https://cybersecuritynews.com/sheetcreep-c-rat-abuses-google-sheets-api/
Hackers Use Free Spotify Premium Hacks on TikTok and Instagram to Spread Vidar Infostealer	https://cybersecuritynews.com/hackers-use-free-spotify-premium-hacks/
Solana FakeFix Campaign Uses 25 Malicious npm and PyPI Packages to Steal Developer Secrets	https://cybersecuritynews.com/solana-fakefix-campaign-uses-25-malicious-npm-and-pypi-packages/
GoFlateLoader Uses Massive PE Overlay to Deliver Lumma, Vidar, and StealC Infostealers	https://cybersecuritynews.com/goflateloader-uses-massive-pe-overlay/

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
DPAPISnoop Tool Extracts CREDHIST Hashes for Offline Windows Credential Recovery	https://cybersecuritynews.com/dpapisnoop-tool-extracts-credhist-hashes/
SecSuite – AI-powered Tool for OSINT, Web and API Security Testing	https://cybersecuritynews.com/secsuite-ai-powered-tool/

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/