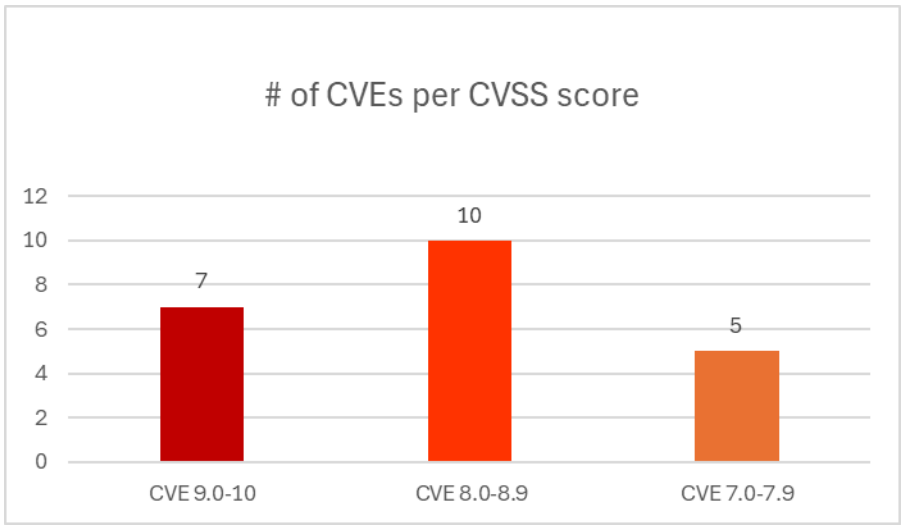
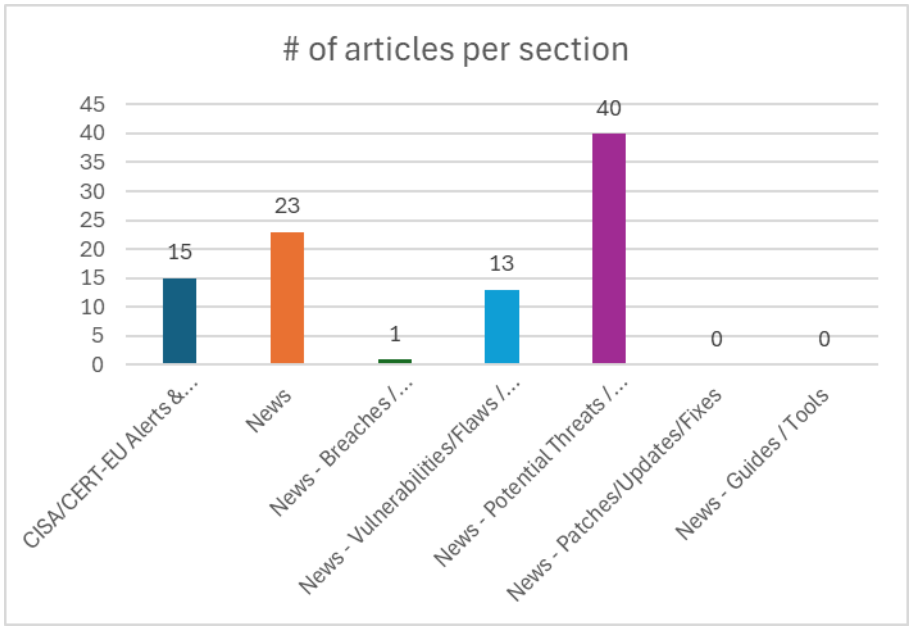
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 29/07/2025 - 01/08/2025





Contents

Common Vulnerabilities and Exposures (CVEs)

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-2025-54381	9,9	BentoML, Python library	Server-Side Request Forgery (SSRF)	In versions 1.4.0 until 1.4.19	https://github.com/bentoml/BentoML/commit/534c3584621da4ab954bdc3d814cc66b95ae5fb8 https://github.com/bentoml/BentoML/security/advisories/GHSA-mrmq-3q62-6cc8
https://nvd.nist.gov/vuln/detail/CVE-2025-44136	9,8	MapTiler	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	MapTiler Tileserver-php v2.1	https://github.com/maptiler/tileserver-php/issues/167 https://github.com/mheranco/CVE-2025-44136
https://nvd.nist.gov/vuln/detail/CVE-2025-46059	9,8	langchain-ai	Improper Control of Generation of Code ('Code Injection')	langchain-ai v0.3.51	https://github.com/Jr61-star/CVEs/blob/main/CVE-2025-46059.md https://github.com/langchain-ai/langchain/issues/30833
https://nvd.nist.gov/vuln/detail/CVE-2025-50738	9,8	The Memos application	Exposure of Sensitive Information to an Unauthorized Actor	The Memos application, up to version v0.24.3	https://github.com/usememos/memos https://github.com/usememos/memos/issues/4707#issuecomment-2898504237
https://nvd.nist.gov/vuln/detail/CVE-2025-54428	9,8	RevelaCode	Insufficiently Protected Credentials	versions below 1.0.1	https://github.com/musombi123/RevelaCode-Backend/commit/95005cf4bacf1b005aef9d4b8e85237c98492d83 https://github.com/musombi123/RevelaCode-Backend/security/advisories/GHSA-m253-qvcr-cr48
https://nvd.nist.gov/vuln/detail/CVE-2025-8426	9,4	Marvell	Improper Limitation of a Pathname to a Restricted Directory	Marvell QConvergeConsole	https://www.zerodayinitiative.com/advisories/ZDI-25-733/

			('Path Traversal')		
https://nvd.nist.gov/vuln/detail/CVE-2025-8264	**9,0**	z-push/z-push-dev	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	z-push/z-push-dev before 2.7.6	https://github.com/Z-Hub/Z-Push/blob/af25a2169a50d6e05a5916d1e8b2b6cd17011c98/src/backend/imap/user_identity.php%23L211C9-L214C25 https://github.com/Z-Hub/Z-Push/pull/161 https://github.com/Z-Hub/Z-Push/pull/161/commits/f981d515a35ac4c303959af21dce880a5db02786 https://security.snyk.io/vuln/SNYK-PHP-ZPUSHZPUSHDEV-10908180 https://xbow.com/blog/xbow-zpush-sqli/
https://nvd.nist.gov/vuln/detail/CVE-2024-42655	**8,8**	NanoMQ	Improper Access Control	NanoMQ v0.21.10	https://github.com/nanomq/nanomq https://github.com/nanomq/nanomq/issues/1782#issuecomment-2171025812 https://github.com/songxpu/bug_report/blob/master/MQTT/NanoMQ/CVE-2024-42655.md
https://nvd.nist.gov/vuln/detail/CVE-2025-53558	**8,8**	ZTE	Use of Weak Credentials	ZXHN-F660T and ZXHN-F660A provided by ZTE Japan K.K.	https://jvn.jp/en/jp/JVN66546573/
https://nvd.nist.gov/vuln/detail/CVE-2025-8320	**8,8**	Tesla	Improper Validation of Specified Quantity in Input	Tesla Wall Connector	https://www.zerodayinitiative.com/advisories/ZDI-25-711/
https://nvd.nist.gov/vuln/detail/CVE-2025-6504	**8,4**	HDP Server	Insufficient Verification of Data Authenticity	HDP Server versions below 4.6.2.2978 on Linux	https://community.progress.com/s/article/DataDirect-Hybrid-Data-Pipeline-Critical-Security-Product-Alert-Bulletin-July-2025---CVE-2025-6504
https://nvd.nist.gov/vuln/detail/CVE-2025-31965	**8,2**	HCL	Authentication Bypass by Primary Weakness	HCL BigFix Remote Control Server WebUI (versions 10.1.0.0248 and lower)	https://support.hcl-software.com/csm?id=kb_article&sysparm_article=KB0122906
https://nvd.nist.gov/vuln/detail/CVE-2025-44137	**8,2**	MapTiler	Improper Limitation of a Pathname	MapTiler Tileserver-php v2.0	https://github.com/maptiler/tileserver-php/issues/167 https://github.com/mheranco/CVE-2025-44137

			to a Restricted Directory ('Path Traversal')		
https://nvd.nist.gov/vuln/detail/CVE-2025-4422	**8,2**	Lenovo	Out-of-bounds Write	Please visit "Lenovo Product Security Advisories and Announcements" webpage for more information about the vulnerability. https://support.lenovo.com/us/en/product_security/home	https://support.lenovo.com/us/en/product_security/home https://support.lenovo.com/us/en/product_security/home https://www.insyde.com/security-pledge/sa-2025007/
https://nvd.nist.gov/vuln/detail/CVE-2025-45346	**8,1**	Bacula-web	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	acula-web before v.9.7.1	https://github.com/bacula-web/bacula-web/commit/ad5d94809f17994a61496ecfec9cd3a16ac14a5f https://github.com/bacula-web/bacula-web/releases/tag/v9.7.1
https://nvd.nist.gov/vuln/detail/CVE-2025-6505	**8,1**	Progress Software's Hybrid Data Pipeline Server on Linux	Improper Authentication	Progress Software's Hybrid Data Pipeline Server on Linux	https://community.progress.com/s/article/DataDirect-Hybrid-Data-Pipeline-Critical-Security-Product-Alert-Bulletin-July-2025---CVE-2025-6505
https://nvd.nist.gov/vuln/detail/CVE-2025-53078	**8,0**	Samsung DMS(Data Management Server)	Deserialization of Untrusted Data	Samsung DMS(Data Management Server)	https://security.samsungda.com/securityUpdates.html
https://nvd.nist.gov/vuln/detail/CVE-2025-33092	**7,8**	IBM	Stack-based Buffer Overflow	IBM Db2 for Linux 12.1.0, 12.1.1, and 12.1.2	https://www.ibm.com/support/pages/node/7240940
https://nvd.nist.gov/vuln/detail/CVE-2025-7675	**7,8**	Autodesk	Out-of-bounds Write		https://www.autodesk.com/trust/security-advisories/adsk-sa-2025-0015
https://nvd.nist.gov/vuln/detail/CVE-2025-28170	**7,6**	Grandstream Networks	Exposure of Information Through Directory Listing	Grandstream Networks GXP1628 <=1.0.4.130	http://grandstream.com https://gist.github.com/Exek1el/928ea6fd06d3b48c1c91cfdc30317d8d

https://nvd.nist.gov/vuln/detail/CVE-2025-6175	**7,2**	DECE Software Geodi	Improper Neutralization of CRLF Sequences ('CRLF Injection')	Geodi: before GEODI Setup 9.0.146	https://www.usom.gov.tr/bildirim/tr-25-0182
https://nvd.nist.gov/vuln/detail/CVE-2025-53080	**7,1**	Samsung DMS(Data Management Server)	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Samsung DMS(Data Management Server)	https://security.samsungda.com/securityUpdates.html

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA and USCG Identify Areas for Cyber Hygiene Improvement After Conducting Proactive Threat Hunt at US Critical Infrastructure Organization		https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-212a
CISA Releases Two Industrial Control Systems Advisories		https://www.cisa.gov/news-events/alerts/2025/07/31/cisa-releases-two-industrial-control-systems-advisories
Rockwell Automation Lifecycle Services with VMware		https://www.cisa.gov/news-events/ics-advisories/icsa-25-212-02
Güralp Systems Güralp FMUS series		https://www.cisa.gov/news-events/ics-advisories/icsa-25-212-01
Thorium Platform Public Availability		https://www.cisa.gov/news-events/alerts/2025/07/31/thorium-platform-public-availability
CISA and USCG Issue Joint Advisory to Strengthen Cyber Hygiene in Critical Infrastructure		https://www.cisa.gov/news-events/alerts/2025/07/31/cisa-and-uscg-issue-joint-advisory-strengthen-cyber-hygiene-critical-infrastructure
CISA and USCG Identify Areas for Cyber Hygiene Improvement After Conducting Proactive Threat Hunt at US Critical Infrastructure Organization		https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-212a
Eviction Strategies Tool Released		https://www.cisa.gov/news-events/alerts/2025/07/30/eviction-strategies-tool-released
CISA Releases Five Industrial Control Systems Advisories		https://www.cisa.gov/news-events/alerts/2025/07/29/cisa-releases-five-industrial-control-systems-advisories
Delta Electronics DTN Soft		https://www.cisa.gov/news-events/ics-advisories/icsa-25-210-03
Samsung HVAC DMS		https://www.cisa.gov/news-events/ics-advisories/icsa-25-210-02
CISA and USCG Identify Areas for Cyber Hygiene Improvement After Conducting Proactive Threat		https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-212a

Hunt at US Critical Infrastructure Organization		
National Instruments LabVIEW		https://www.cisa.gov/news-events/ics-advisories/icsa-25-210-01
CISA Releases Part One of Zero Trust Microsegmentation Guidance		https://www.cisa.gov/news-events/alerts/2025/07/29/cisa-releases-part-one-zero-trust-microsegmentation-guidance
CISA and Partners Release Updated Advisory on Scattered Spider Group		https://www.cisa.gov/news-events/alerts/2025/07/29/cisa-and-partners-release-updated-advisory-scattered-spider-group

News

Σύντομη περιγραφή / Τίτλος	URL
CISA Open-sources Malware and Forensic Analysis Tool Thorium to Public Availability	https://cybersecuritynews.com/thorium-tool/
17K+ SharePoint Servers Exposed to Internet – 840 Servers Vulnerable to 0-Day Attacks	https://cybersecuritynews.com/sharepoint-servers-exposed-to-internet/
Chinese Companies Linked With Hackers Filed Patents Over 10+ Forensics and Intrusion Tools	https://cybersecuritynews.com/chinese-hackers-filed-patents/
Lenovo IdeaCentre and Yoga Laptop BIOS Vulnerabilities Let Attackers Execute Arbitrary Code	https://cybersecuritynews.com/lenovo-ideacentre-and-yoga-laptop-bios-vulnerabilities/
Hacker Arrested for Stealing Users Personal Data from Spanish Banks	https://cybersecuritynews.com/hacker-arrested-for-stealing-spanish-banks/
Google Project Zero to Publicly Announce Vulnerabilities Within a Week of Reporting Them	https://cybersecuritynews.com/google-project-zero-vulnerability-disclosure/
UNC2891 Threat Actors Hacked ATM Networks Using 4G Raspberry Pi Device	https://cybersecuritynews.com/atm-network-hacked-using-raspberry-pi/
Bangalore Techie Arrested in Connection With the $44 Million CoinDCX Hack	https://cybersecuritynews.com/bangalore-techie-arrested-coindcx/
ChatGPT, Gemini, GenAI Tools Vulnerable to Man-in-the-Prompt Attacks	https://cybersecuritynews.com/man-in-the-prompt-attack/
Palo Alto Networks to Acquire CyberArk in $25 Billion Deal	https://cybersecuritynews.com/palo-alto-networks-acquire-cyberark/
5 Email Attacks SOCs Cannot Detect Without A Sandbox	https://cybersecuritynews.com/5-email-attacks-socs-cannot-detect-without-a-sandbox/
Critical SonicWall SSL VPN Vulnerability Let Attackers Trigger DoS Attack on Firewalls	https://cybersecuritynews.com/sonicwall-ssl-vpn-dos-vulnerability/
Global Authorities Shared IoCs and TTPs of Scattered Spider Behind Major VMware ESXi Ransomware Attacks	https://cybersecuritynews.com/scattered-spider-esxi-ransomware-attacks/
ChatGPT Agent Bypasses Cloudflare “I am not a robot” Verification Checks	https://cybersecuritynews.com/chatgpt-agent-bypasses-cloudflare/
Hackers Exploiting SAP NetWeaver Vulnerability to Deploy Auto-Color Linux Malware	https://cybersecuritynews.com/sap-netweaver-vulnerability-exploited-malware/
Enterprise LLMs Under Risk: How Simple Prompts Can Lead to Major Breaches	https://cybersecuritynews.com/llms-risk-prompts-lead-to-breaches/

Microsoft Details Defence Techniques Against Indirect Prompt Injection Attacks	https://cybersecuritynews.com/indirect-prompt-injection-mitigations/
AccuKnox Partners With CyberKnight To Deliver Zero Trust Security For A Leading Global Bank In The UAE.	https://cybersecuritynews.com/accuknox-partners-with-cyberknight-to-deliver-zero-trust-security-for-a-leading-global-bank-in-the-uae/
Orange Hit by Cyberattack – A French Telecom Giant's Internal Systems Hacked	https://cybersecuritynews.com/orangetelecom-hit-by-cyberattack/
PyPI Warns of New Phishing Attack Targeting Developers With Fake PyPI Site	https://cybersecuritynews.com/phishing-attack-with-fake-pypi-site/
Linux 6.16 Released – Optimized for Better Performance and Networking	https://cybersecuritynews.com/linux-6-16-released/
Apple's New Containerization Feature Allows Kali Linux Integration on macOS	https://cybersecuritynews.com/apples-containerization-feature-macos/
GitHub Outage Disrupts Core Services Globally for Users	https://cybersecuritynews.com/github-outage-disrupts-core-services/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Threat Actors Allegedly Claim Access to Nokia's Internal Network	https://cybersecuritynews.com/nokia-internal-systems-breach/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Critical SUSE Manager Vulnerability Let Attackers Execute Arbitrary Commands as Root	https://cybersecuritynews.com/suse-manager-vulnerability/
Critical CrushFTP 0-Day RCE Vulnerability Technical Details and PoC Released	https://cybersecuritynews.com/crushftp-0-day-technical-details-poc-released/
OAuth2-Proxy Vulnerability Enables Authentication Bypass by Manipulating Query Parameters	https://cybersecuritynews.com/oauth2-proxy-authentication-bypass/
AI Vibe Coding Platform Hacked – Logic Flaw Exposes Private App Access	https://cybersecuritynews.com/ai-vibe-coding-platform-hacked/
WordPress Theme RCE Vulnerability Actively Exploited to Take Full Site Control	https://cybersecuritynews.com/wordpress-theme-rce-vulnerability-exploited/
BeyondTrust Privilege Management for Windows Vulnerability Let Attackers Escalate Privileges	https://cybersecuritynews.com/beyondtrust-privilege-management-for-windows/
Chrome High-Severity Vulnerabilities Allow Memory Manipulation and Arbitrary Code Execution	https://cybersecuritynews.com/chrome-security-update-138/
Critical CodeIgniter Vulnerability Exposes Million of Webapps to File Upload Attacks	https://cybersecuritynews.com/codeigniter-vulnerability/
SonicWall SMA100 Series N-day Vulnerabilities Technical Details Revealed	https://cybersecuritynews.com/sonicwall-n-day-vulnerabilities/
Gemini CLI Vulnerability Allows Hackers to Execute Malicious Commands on Developer Systems	https://cybersecuritynews.com/gemini-cli-vulnerability/
CISA Warns of PaperCut RCE Vulnerability Exploited in Attacks	https://cybersecuritynews.com/papercut-rce-vulnerability-exploited/
Critical macOS 'Sploitlight' Vulnerability Let Attackers Steal Private Data of Files Bypassing TCC	https://cybersecuritynews.com/macos-sploitlight-vulnerability/
CISA Warns of Cisco Identity Services Engine Vulnerability Exploited in Attacks	https://cybersecuritynews.com/cisco-identity-services-engine-vulnerability/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Unit 42 Unveils Attribution Framework to Classify Threat Actors Based on Activity	https://cybersecuritynews.com/unit-42-unveils-attribution-framework/
Threat Actors Embed Malicious RMM Tools to Gain Silent Initial Access to Organizations	https://cybersecuritynews.com/threat-actors-embed-malicious-rmm-tools/
Navigating APTs – Singapore's Cautious Response to State-Linked Cyber Attacks	https://cybersecuritynews.com/navigating-apts-singapores-cautious-response/
Silver Fox Hackers Using Weaponized Google Translate Tools to Deploy Windows Malware	https://cybersecuritynews.com/silver-fox-hackers-using-weaponized-google-translate/
Anubis Ransomware Attacking Android and Windows Users to Encrypt Files and Steal Login Credentials	https://cybersecuritynews.com/anubis-ransomware-attacking-android-and-windows-users/
First AI-Powered Malware LAMEHUG Attacking Organizations With Compromised Official Email Account	https://cybersecuritynews.com/first-ai-powered-malware-lamehug-attacking-organizations/
New Banking Malware DoubleTrouble Attacking Users Via Phishing Sites To Steal Banking Credentials	https://cybersecuritynews.com/new-banking-malware-doubletrouble-attacking-users/
Chinese Silk Typhoon Hackers Filed 10+ Patents for Highly Intrusive Hacking Tools	https://cybersecuritynews.com/chinese-silk-typhoon-hackers-filed-10-patents/
NOVABLIGHT as Educational Tool Attacking Users to Steal Login Credentials and Compromise Wallets	https://cybersecuritynews.com/novablight-as-educational-tool-attacking-users/
Ransomware Groups Using TrickBot Malware to Exfiltrate US$724 Million in Cryptocurrency	https://cybersecuritynews.com/ransomware-groups-using-trickbot-malware/
North Korean APT Hackers Poison CI/CD Pipelines To Exfiltrate Sensitive Data	https://cybersecuritynews.com/north-korean-apt-hackers-poison-ci-cd-pipelines/
Hackers Delivering Cobalt Strike Beacon Leveraging GitHub and Social Media	https://cybersecuritynews.com/hackers-delivering-cobalt-strike-beacon/
Researchers Detailed North Korean Threat Actors Technical Strategies to Uncover Illicit Access	https://cybersecuritynews.com/north-korean-threat-actors-technical-strategies/
Threat Actors Weaponizes LNK Files to Deploy RedLoader Malware on Windows Systems	https://cybersecuritynews.com/threat-actors-deploy-redloader-malware-on-windows/
New Spear Phishing Attack Delivers VIP Keylogger via EMAIL Attachment	https://cybersecuritynews.com/new-spear-phishing-attack-delivers-vip-keylogger/
LLM Honeypot's Can Trick Threat Actors to Leak Binaries and Known Exploits	https://cybersecuritynews.com/llm-honeypots-can-trick-threat-actors/
Microsoft SharePoint Server 0-Day Hack Hits African Treasury, Companies, and University	https://cybersecuritynews.com/microsoft-sharepoint-server-0-day-hack/
APT Hackers Attacking Maritime and Shipping Industry to Launch Ransomware Attacks	https://cybersecuritynews.com/apt-hackers-attacking-maritime-and-shipping-industry/
Gunra Ransomware New Linux Variant Runs Up To 100 Encryption Threads With New Partial Encryption Feature	https://cybersecuritynews.com/gunra-ransomware-new-linux-variant/
Qilin Ransomware Leverages TPwSav.sys Driver to Disable EDR Security Measures	https://cybersecuritynews.com/qilin-ransomware-leverages-tpwsav-sys-driver/

New JSCEAL Attack Targeting Crypto App Users To Steal Credentials and Wallets	https://cybersecuritynews.com/new-jsceal-attack-targeting-crypto-app-users/
Free Decryptor Released for AI-Assisted FunkSec Ransomware	https://cybersecuritynews.com/ai-assisted-funksec-ransomware/
CISA and FBI Shared Tactics, Techniques, and Procedures of Scattered Spider Hacker Group	https://cybersecuritynews.com/cisa-and-fbi-shared-ttps-of-scattered-spider/
Qilin Ransomware Gain Traction Following Legal Assistance Option for Ransomware Affiliates	https://cybersecuritynews.com/qilin-ransomware-gain-traction/
BulletProof Hosting Provider Qwins Ltd Fueling Global Malware Campaigns	https://cybersecuritynews.com/bulletproof-hosting-provider-qwins-ltd/
0bj3ctivityStealer's Execution Chain Unveiled With It's New Capabilities and Exfiltration Techniques	https://cybersecuritynews.com/0bj3ctivitystealers-execution-chain/
ToxicPanda Android Banking Malware Infected 4500+ Devices to Steal Banking Credentials	https://cybersecuritynews.com/toxicpanda-android-banking-malware/
New XWorm V6 Variant's With Anti-Analysis Capabilities Attacking Windows Users in The Wild	https://cybersecuritynews.com/new-xworm-v6-variants-with-anti-analysis-capabilities/
Lazarus Subgroup 'TraderTraitor' Attacking Cloud Platforms and Poisoning Supply Chains	https://cybersecuritynews.com/lazarus-subgroup-tradertraitor-attacking-cloud-platforms/
Threat Actors Weaponize LNK Files With New REMCOS Variant That Bypasses AV Engines	https://cybersecuritynews.com/threat-actors-weaponize-lnk-files-with-new-remcos/
Lumma Password Stealer Attack Infection Chain and Its Escalation Tactics Uncovered	https://cybersecuritynews.com/lumma-password-stealer-attack-infection-chain/
Lionishackers Threat Actors Exfiltrating and Selling Corporate Databases on Dark Web	https://cybersecuritynews.com/lionishackers-threat-actors/
Threat Actors Attacking Fans and Teams of Belgian Grand Prix With Phishing Campaigns	https://cybersecuritynews.com/threat-actors-attacking-fans-of-belgian-grand-prix/
ArmouryLoader Bypassing System Security Protections and Inject Malicious Codes	https://cybersecuritynews.com/armouryloader-bypassing-system-security-protections/
Want To Detect Incidents Before It's Too Late? You Need Threat Intelligence	https://cybersecuritynews.com/want-to-detect-incidents-before-its-too-late-you-need-threat-intelligence/
Chinese Hackers Weaponizes Software Vulnerabilities to Compromise Their Targets	https://cybersecuritynews.com/chinese-hackers-weaponizes-software-vulnerabilities/
UNC3886 Actors Know for Exploiting 0-Days Attacking Singapore's Critical Infrastructure	https://cybersecuritynews.com/unc3886-actors-know-for-exploiting-0-days/
npm 'is' Package With 2.8M Weekly Downloads Weaponized to Attack Developers	https://cybersecuritynews.com/npm-is-package-with-2-8m-weekly-downloads-weaponized/
Telegram Based Raven Stealer Malware Steals Login Credentials, Payment Data and Autofill Information	https://cybersecuritynews.com/telegram-based-raven-stealer-malware/
Hackers Attacking IIS Servers With New Web Shell Script to Gain Complete Remote Control	https://cybersecuritynews.com/hackers-attacking-iis-servers-with-new-web-shell-script/

Guides / Tools

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.

[3]. Τα CVEs που αφορούν Wordpress plugins θα εμφανίζονται σε ξεχωριστή ενότητα (1.1) σε περιόδους που η εμφάνισή τους είναι ιδιαίτερα αυξημένη.

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/