NATIONAL CYBERSECURITY AUTHORITY GR

CVEs Alerts

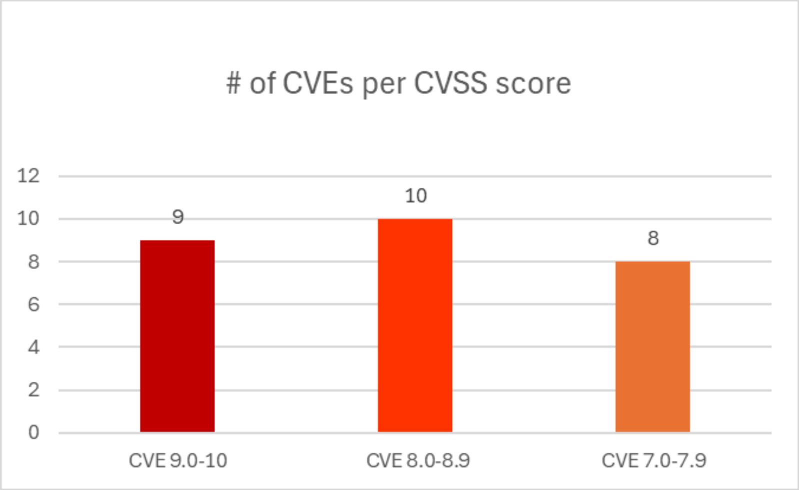
CVEs, CISA/CERT-EU
Alerts
Advisories
& News

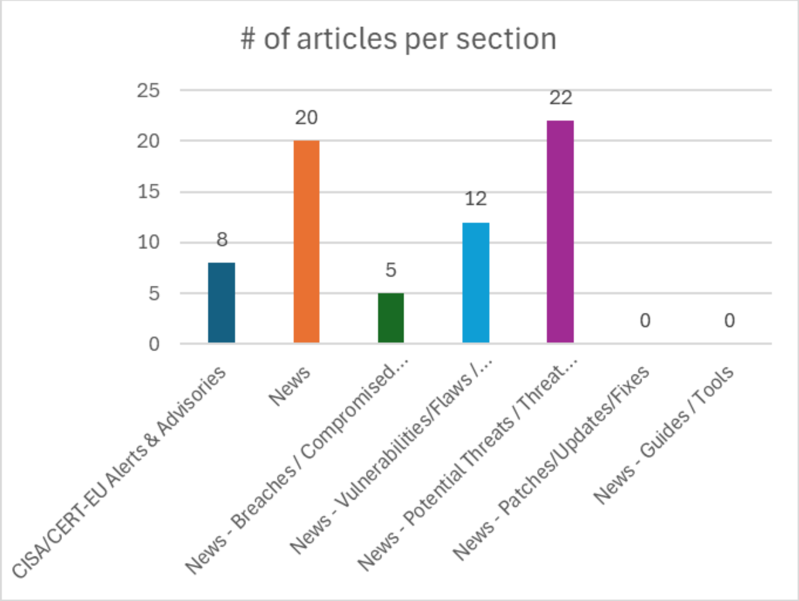
Newsletter on system vulnerabilities and cybersecurity news

Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 25/07/2025 - 29/07/2025





Contents

Common Vulnerabilities and Exposures (CVEs)

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-2025-54381	**9,9**	BentoML is a Python library	Server-Side Request Forgery (SSRF)	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-2025-30125	**9,8**	Marbella KR8s Dashcam	Use of Hard-coded Credentials	Marbella KR8s Dashcam FF 2.0.8 devices	https://geochen.medium.com/marbella-dashcam-ab40ca41ade https://github.com/geo-chen/Marbella/ https://github.com/geo-chen/Marbella/blob/main/README.md#finding-1---cve-2025-30125-same-default-credentials-and-limited-password-combinations https://makagps.com/ https://www.protiviti.com/sg-en/blogs/6259-8-character-password-still-dead
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 v2.0	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 was discovered to contain an indirect prompt injection vulnerability in the GmailToolkit component	https://github.com/Jr61-star/CVEs/blob/main/CVE-2025-46059.md https://github.com/langchain-ai/langchain-community/issues/217#issuecomment-3144824471 https://github.com/langchain-ai/langchain/issues/30833 https://python.langchain.com/docs/security/
https://nvd.nist.gov/vuln/detail/CVE-2025-46199	**9,8**	grav CMS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	grav v.1.7.48	https://rapid-echo-f9c.notion.site/Grav-XSS-25-04-21-1dcaf8998a078001a2eff3dc47974d6d?pvs=4 https://tyojong.tistory.com/2
https://nvd.nist.gov/vuln/detail/CVE-2025-50738	**9,8**	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-2025-8169	**9,8**	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	D-Link DIR-513 1.10	https://github.com/InfiniteLin/Lin-s-CVEdb/blob/main/DIR-513/formSetWanPPPoE.md VulDB https://vuldb.com/?ctiid.317583 https://vuldb.com/?id.317583 https://vuldb.com/?submit.620817 https://www.dlink.com/

https://nvd.nist.gov/vuln/detail/CVE-2025-8184	9,8	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	D-Link DIR-513 up to 1.10	https://github.com/InfiniteLin/Lin-s-CVEdb/blob/main/DIR-513/formSetWanPPTP.md https://vuldb.com/?ctiid.317597 https://vuldb.com/?id.317597 https://vuldb.com/?submit.622222 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-30135	9,4	IROAD Dashcam FX2	Missing Authentication for Critical Function	IROAD Dashcam FX2	https://github.com/geo-chen/IROAD?tab=readme-ov-file#finding-13---cve-2025-30135-locking-owner-out-of-device-dos https://github.com/geo-chen/IROAD?tab=readme-ov-file#finding-8-dumping-files-over-http-and-rtsp-without-authentication https://www.iroadau.com.au/downloads/
https://nvd.nist.gov/vuln/detail/CVE-2024-42655	8,8	NanoMQ v0.21.10	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-2025-54528	8,8	JetBrains	Cross-Site Request Forgery (CSRF)	JetBrains TeamCity before 2025.07	https://www.jetbrains.com/privacy-security/issues-fixed/
https://nvd.nist.gov/vuln/detail/CVE-2025-8131	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda AC20 16.03.08.05	https://github.com/Thir0th/Thir0th-CVE/blob/main/Tenda_AC20_V16.03.08.05_has_a_stack_overflow.md https://vuldb.com/?ctiid.317527 https://vuldb.com/?id.317527 https://vuldb.com/?submit.619769 https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-8137	8,8	TOTOLINK	Improper Restriction of Operations within the Bounds of a Memory Buffer	TOTOLINK A702R 4.0.0-B20230721.1521	https://github.com/panda666-888/vuls/blob/main/totolink/a702r/formIpQoS.md https://vuldb.com/?ctiid.317533 https://vuldb.com/?id.317533 https://vuldb.com/?submit.620483 https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2025-8159	8,8	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	D-Link DIR-513 1.0	https://github.com/boyslikesports/vul/blob/main/formLanguageChange.md https://vuldb.com/?ctiid.317573 https://vuldb.com/?id.317573 https://vuldb.com/?submit.620604 https://www.dlink.com/

https://nvd.nist.gov/vuln/detail/CVE-2025-8160	**8,8**	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda AC20 up to 16.03.08.12	https://github.com/CH13hh/cve/blob/main/tenda1.md VulDB https://vuldb.com/?ctiid.317574 https://vuldb.com/?id.317574 https://vuldb.com/?submit.620625 https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-8170	**8,8**	TOTOLINK	Improper Restriction of Operations within the Bounds of a Memory Buffer	TOTOLINK T6 4.1.5cu.748_B20211015	https://github.com/AnduinBrian/Public/blob/main/Totolink%20T6/Vuln/9.md VulDB Exploit Third Party Advisory https://github.com/AnduinBrian/Public/blob/main/Totolink%20T6/Vuln/9.md#poc https://vuldb.com/?ctiid.317584 https://vuldb.com/?id.317584 https://vuldb.com/?submit.620834 https://www.totolink.net/
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-2025-54378	**8,3**	HAX CMS	Improper Authorization	HAX CMS	https://github.com/haxtheweb/haxcms-nodejs/commit/5826e9b7f3d8c7c7635411768b86b199fad36969 GitHub https://github.com/haxtheweb/haxcms-php/commit/24d30222481ada037597c4d7c0a51a1ef7af6cfd https://github.com/haxtheweb/issues/security/advisories/GHSA-9jr9-8ff3-m894
https://nvd.nist.gov/vuln/detail/CVE-2025-52453	**8,2**	Salesforce Tableau	Server-Side Request Forgery (SSRF)	Tableau Server: before 2025.1.3, before 2024.2.12, before 2023.3.19	https://help.salesforce.com/s/articleView?id=005105043&type=1
https://nvd.nist.gov/vuln/detail/CVE-2025-6637	**7,8**	Autodesk	Out-of-bounds Write	Autodesk	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-2024-49342	**7,5**	IBM Informix Dynamic Server	Improper Restriction of Excessive Authentication Attempts	IBM Informix Dynamic Server 12.10 and 14.10	https://www.ibm.com/support/pages/node/7240777
https://nvd.nist.gov/vuln/detail/CVE-2025-36010	**7,5**	IBM	Deadlock	IBM Db2 for Linux 12.1.0, 12.1.1, and 12.1.2	https://www.ibm.com/support/pages/node/7240951

https://nvd.nist.gov/vuln/detail/CVE-2025-36071	**7,5**	IBM Db2	Missing Release of Resource after Effective Lifetime	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5.0 through 11.5.9 and 12.1.0 through 12.1.2	https://www.ibm.com/support/pages/node/7240955
https://nvd.nist.gov/vuln/detail/CVE-2025-53715	**7,5**	TP-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	TP-Link TL-WR841N V11	https://www.tp-link.com/us/support/faq/4569/
https://nvd.nist.gov/vuln/detail/CVE-2025-8136	**7,5**	TOTOLINK	Improper Restriction of Operations within the Bounds of a Memory Buffer	TOTOLINK A702R 4.0.0-B20230721.1521	https://github.com/panda666-888/vuls/blob/main/totolink/a702r/formFilter.md https://vuldb.com/?ctiid.317532 https://vuldb.com/?id.317532 https://vuldb.com/?submit.620482 https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2025-8182	**7,4**	Tenda	Weak Password Requirements	Tenda AC18 15.03.05.19	https://vuldb.com/?ctiid.317596 https://vuldb.com/?id.317596 VulDB https://vuldb.com/?submit.621977 https://www.notion.so/23a54a1113e7802abfabf1275a555f48 https://www.tenda.com.cn/

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Releases Five Industrial Control Systems Advisories	▪ ICSA-25-210-01 National Instruments LabVIEW ▪ ICSA-25-210-02 Samsung HVAC DMS ▪ ICSA-25-210-03 Delta Electronics DTN Soft ▪ ICSA-24-158-04 Johnson Controls Software House iStar Pro Door Controller (Update A) ▪ ICSA-24-338-06 Fuji Electric Tellus Lite V-Simulator (Update A)	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
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
CISA Adds Three Known Exploited Vulnerabilities to Catalog	▪ CVE-2025-20281 Cisco Identity Services Engine Injection Vulnerability ▪ CVE-2025-20337 Cisco Identity Services Engine Injection Vulnerability ▪ CVE-2023-2533 PaperCut NG/MF Cross-Site Request Forgery (CSRF) Vulnerability	https://www.cisa.gov/news-events/alerts/2025/07/28/cisa-adds-three-known-exploited-vulnerabilities-catalog
Vulnerability Summary for the Week of July 28, 2025		https://www.cisa.gov/news-events/bulletins/sb25-216

News

Σύντομη περιγραφή / Τίτλος	URL
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/
Orange Hit by Cyberattack – A French Telecom Giant’s Internal Systems Hacked	https://cybersecuritynews.com/orangetelecom-hit-by-cyberattack/
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/
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/
GitHub Outage Disrupts Core Services Globally for Users	https://cybersecuritynews.com/github-outage-disrupts-core-services/
Hackers Allegedly Destroyed Aeroflot Airlines’ IT Infrastructure in Year-Long Attack	https://cybersecuritynews.com/aeroflot-airlines-cyberattack/
Oyster Malware as PuTTY, KeyPass Attacking IT Admins by Poisoning SEO Results	https://cybersecuritynews.com/oyster-malware-as-putty/
Leak Zone Dark Web Forum Database Exposes 22 Million Users’ IP Addresses and Locations	https://cybersecuritynews.com/leak-zone-dark-web-forum-database-exposed/
Arizona Woman Sentenced for Helping North Korean IT Workers by Operating Laptop Farm	https://cybersecuritynews.com/arizona-woman-sentenced/
Weekly Cybersecurity News Recap : Sharepoint 0-day, Vmware Exploitation, Threats and Cyber Attacks	https://cybersecuritynews.com/weekly-cybersecurity-news-recap-report/
Hackers Compromised Official Gaming Mouse Software to Deliver Windows-based Xred Malware	https://cybersecuritynews.com/gaming-mouse-software-compromised/
Infamous BreachForums Is Back Online With All Old Accounts and Posts Restored	https://cybersecuritynews.com/breachforums-back-online/
Microsoft Probes Leak in Early Alert System as Chinese Hackers Exploit SharePoint Vulnerabilities	https://cybersecuritynews.com/microsoft-early-alert-sharepoint-vulnerabilities/
New VOIP-Based Botnet Attacking Routers Configured With Default Password	https://cybersecuritynews.com/voip-based-botnet-attacking-routers/
Microsoft 365 Admin Center Outage Blocks Access for Admins Worldwide	https://cybersecuritynews.com/microsoft-365-admin-center-outag/
Bulletproof Hosting Provider Aeza Group Shifting Their Infrastructure to New Autonomous System	https://cybersecuritynews.com/bulletproof-hosting-provider-shifting-infrastructure/
Fire Ant Hackers Exploiting Vulnerabilities in VMware ESXi and vCenter to Infiltrate Organizations	https://cybersecuritynews.com/vmware-esxi-and-vcenter-exploited/
Hackers Exploiting Sharepoint 0-day Vulnerability to Deploy Warlock Ransomware	https://cybersecuritynews.com/sharepoint-0-day-ransomware-attack/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Threat Actors Allegedly Claiming Breach of Airpay Payment Gateway	https://cybersecuritynews.com/airpay-payment-gateway-breach/
Women’s Dating App Tea Exposes Selfie Images of 13,000 Users	https://cybersecuritynews.com/womens-dating-app-tea-exposes-selfie-images/
Hackers Compromise Intelligence Website Used by CIA and Other Agencies	https://cybersecuritynews.com/cia-intelligence-website-compromised/
Allianz Life Insurance Data Breach – 1.4 Million Customers’ Data at Risk	https://cybersecuritynews.com/allianz-life-insurance-data-breach/
BlackSuit Ransomware’s Data Leak and Negotiation Portal Seized	https://cybersecuritynews.com/blacksuit-ransomware-portal-seized/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
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/
UNC3886 Hackers Exploiting 0-Days in VMware vCenter/ESXi, Fortinet FortiOS, and Junos OS	https://cybersecuritynews.com/unc3886-hackers-exploiting-0-days/
New “ToolShell” Exploit Chain Attacking SharePoint Servers to Gain Complete Control	https://cybersecuritynews.com/toolshell-exploit-chain-sharepoint-servers/
LG Innotek Camera Vulnerabilities Let Attackers Gain Administrative Access	https://cybersecuritynews.com/lg-innotek-camera-vulnerabilities/
Critical Salesforce Tableau Vulnerabilities Let Attackers Execute Code Remotely	https://cybersecuritynews.com/salesforce-tableau-vulnerabilities/
Microsoft Copilot Rooted to Gain Unauthorized Root Access to its Backend System	https://cybersecuritynews.com/microsoft-copilot-rooted/
Multiple Vulnerabilities in Tridium Niagara Framework Let Attacker to Collect Sensitive Data from the Network	https://cybersecuritynews.com/multiple-vulnerabilities-in-tridium-niagara-framework/
Critical VMware Tools VGAuth Vulnerabilities Enable Full System Access for Attackers	https://cybersecuritynews.com/vgauth-flaws-of-vmware-tools/
Hackers Injected Destructive System Commands in Amazon’s AI Coding Agent	https://cybersecuritynews.com/amazons-ai-coding-agent-exploited/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
ArmouryLoader Bypassing System Security Protections and Inject Malicious Codes	https://cybersecuritynews.com/armouryloader-bypassing-system-security-protections/
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/
Renting Android Malware With 2FA Interception, AV Bypass is Getting Cheaper Now	https://cybersecuritynews.com/renting-android-malware-with-2fa-interception/
Atomic macOS Stealer Comes With New Backdoor to Enable Remote Access	https://cybersecuritynews.com/atomic-macos-stealer-comes-with-new-backdoor/
Muddled Libra Actors Attacking Organizations Call Centers for Initial Infiltration	https://cybersecuritynews.com/muddled-libra-actors-attacking-organizations/
Laundry Bear Infrastructure, Key Tactics and Procedures Uncovered	https://cybersecuritynews.com/laundry-bear-infrastructure/
New SHUYAL Attacking 19 Popular Browsers to Steal Login Credentials	https://cybersecuritynews.com/new-shuyal-attacking-19-popular-browsers/
Beware of Fake Error Pages That Linux and Windows Systems With Platform-Specific Malware	https://cybersecuritynews.com/beware-of-fake-error-pages-that-linux-and-windows-systems/
New Gunra Ransomware Attacking Windows Computers to Encrypt Files and Deletes Shadow Copies	https://cybersecuritynews.com/new-gunra-ransomware-attacking-windows-computers/
Hackers Trick Victims into Downloading Weaponized .HTA Files to Install Red Ransomware	https://cybersecuritynews.com/weaponized-hta-files-to-install-red-ransomware/
Hackers Leverage Google Forms Surveys to Trick Victims into Stealing Cryptocurrency	https://cybersecuritynews.com/hackers-leverage-google-forms-surveys/
New Phishing Attack Mimics Facebook Login Page to Steal Credentials	https://cybersecuritynews.com/new-phishing-attack-mimics-facebook-login-page/
Malicious Android Apps Mimic as Popular Indian Banking Apps Steal Login Credentials	https://cybersecuritynews.com/malicious-android-apps-mimic-as-popular-indian-banking-apps/
New Malware Attack Leverages YouTube Channels and Discord to Harvest Credentials from Computer	https://cybersecuritynews.com/new-malware-attack-leverages-youtube-channels-and-discord/
New CastleLoader Attack Using Cloudflare-Themed Clickfix Technique to Infect Windows Computers	https://cybersecuritynews.com/castleloader-attack-using-cloudflare-themed-clickfix-technique/

Hive0156 Hackers Attacking Government and Military Organizations to Deploy Remcos RAT	https://cybersecuritynews.com/hive0156-hackers-attacking-government/
Rise in Phishing Activity Using Spoofed SharePoint Domains With Sneaky2FA Techniques	https://cybersecuritynews.com/rise-in-phishing-activity-using-spoofed-sharepoint-domains/
Elephant APT Group Attacking Defense Industry Leveraging VLC Player, and Encrypted Shellcode	https://cybersecuritynews.com/elephant-apt-group-attacking-defense-industry/

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/