NATIONAL CYBERSECURITY AUTHORITY GR

CVEs Alerts

CVEs, CISA/CERT-EU Alerts Advisories & News

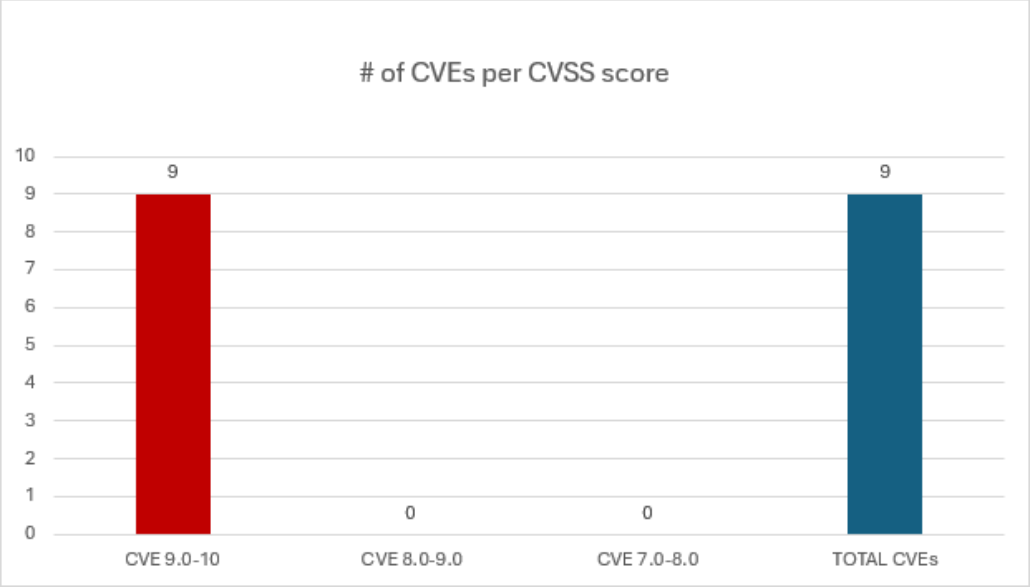
11/04/2025 -15/04/2025

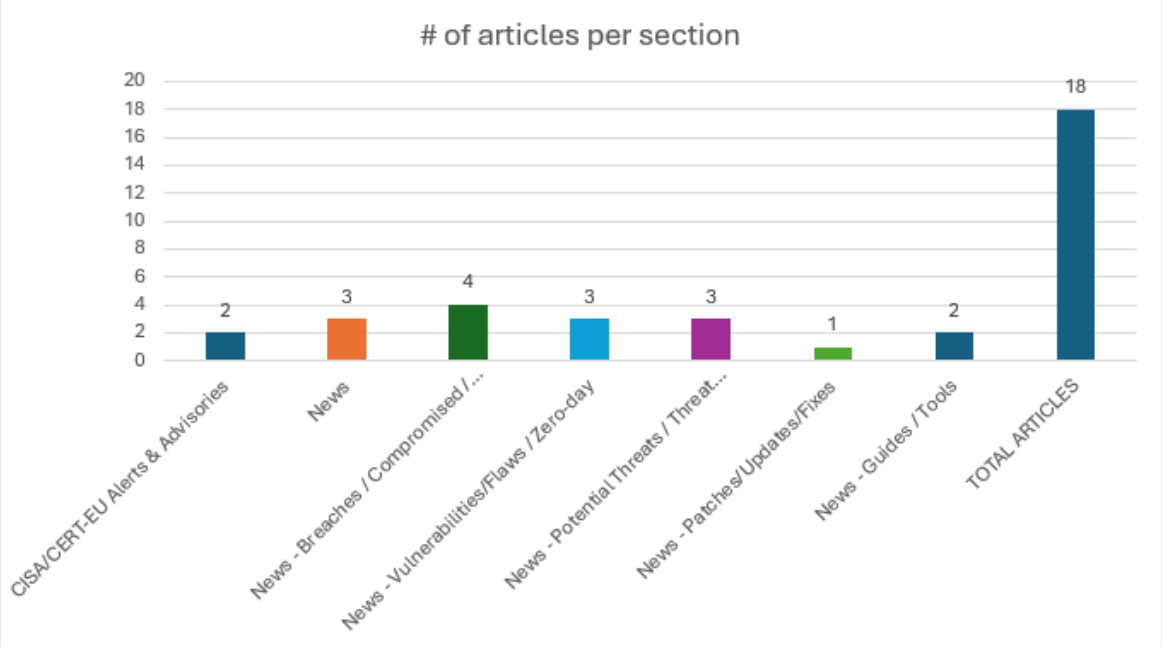
Newsletter on system vulnerabilities and cybersecurity news

Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 11/04/2025 - 15/04/2025





Contents

Common Vulnerabilities and Exposures (CVEs)

URL ευπάθειας (NIST NVD)	CVSSv4	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	Συσκευές/Εκδόσεις που ΔΕΝ επηρεάζο-νται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2022-46642	**9,9**	Dlink	command injection	Dir-846 Dir-846 Firmware	n/a	https://github.com/CyberUnicornIoT/IoTvuln/blob/main/d-link/dir-846/D-Link%20dir-846%20SetAutoUpgradeInfo%20command%20injection%20vulnerability.md
https://www.cve.org/CVERecord?id=CVE-2023-36434	**9,8**	Microsoft	Windows IIS Server Elevation of Privilege Vulnerability	Windows 10 1507 Windows 10 1607 Windows 10 1809 Windows 10 21h2 Windows 10 22h2 Windows 11 21h2 Windows 11 22h2 Windows Server 2008 Windows Server 2012 Windows Server 2016 Windows Server 2019 Windows Server 2022	n/a	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36434
https://nvd.nist.gov/vuln/detail/CVE-2022-47939	**9,8**	Linux kernel		5.15 through 5.19 before 5.19.2.	n/a	http://www.openwall.com/lists/oss-security/2022/12/23/10 Mailing List Third Party Advisory http://www.openwall.com/lists/oss-security/2022/12/23/10 Mailing List Third Party Advisory https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.19.2 Mailing List Patch Vendor Advisory https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.19.2 Mailing List Patch Vendor Advisory

						https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=cf6531d98190fa2cf92a6d8bbc8af0a4740a223c Mailing List Patch Vendor Advisory https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=cf6531d98190fa2cf92a6d8bbc8af0a4740a223c Mailing List Patch Vendor Advisory https://github.com/torvalds/linux/commit/cf6531d98190fa2cf92a6d8bbc8af0a4740a223c Patch Third Party Advisory https://github.com/torvalds/linux/commit/cf6531d98190fa2cf92a6d8bbc8af0a4740a223c Patch Third Party Advisory https://www.secpod.com/blog/zero-day-server-message-block-smb-server-in-linux-kernel-5-15-has-a-critical-vulnerability-patch-ksmbd-immediately/ Third Party Advisory https://www.secpod.com/blog/zero-day-server-message-block-smb-server-in-linux-kernel-5-15-has-a-critical-vulnerability-patch-ksmbd-immediately/ Third Party Advisory https://www.zerodayinitiative.com/advisories/ZDI-22-1690/ Third Party Advisory VDB Entry https://www.zerodayinitiative.com/advisories/ZDI-22-1690/
https://nvd.nist.gov/vuln/detail/CVE-2022-47949	**9,8**	Nintendo	buffer overflow	Mario Kart 7 before 1.2, Mario Kart 8, Mario Kart 8 Deluxe before 2.1.0, ARMS before 5.4.1, Splatoon, Splatoon 2 before 5.5.1, Splatoon 3 before late 2022, Super Mario Maker 2 before 3.0.2, and Nintendo Switch Sports before late 2022	n/a	https://github.com/PabloMK7/ENLBufferPwn Exploit Third Party Advisory https://github.com/PabloMK7/ENLBufferPwn

https://nvd.nist.gov/vuln/detail/CVE-2022-4221	**9,8**	Asus NAS-M25	Improper Neutralization of Special Elements used in an OS Command	NAS-M25: through 1.0.1.7	n/a	https://onekey.com/blog/security-advisory-asus-m25-nas-vulnerability/
https://nvd.nist.gov/vuln/detail/CVE-2022-46600	**9,8**	Trendnet	stack overflow	Tew-755ap Tew-755ap Firmware	n/a	https://brief-nymphea-813.notion.site/Vul4-TEW755-injection-set_sta_enrollee_pin_24g-f91b4c03489146af804fe59a3f44d0d3 Exploit Third Party Advisory https://brief-nymphea-813.notion.site/Vul4-TEW755-injection-set_sta_enrollee_pin_24g-f91b4c03489146af804fe59a3f44d0d3
https://nvd.nist.gov/vuln/detail/CVE-2022-4606	**9,8**	flatpressblog/flatpress	PHP Remote File Inclusion	prior to 1.3	n/a	https://github.com/flatpressblog/flatpress/commit/c30d52b28483e1e512d0d81758d4c149f02b4068 Patch Third Party Advisory https://github.com/flatpressblog/flatpress/commit/c30d52b28483e1e512d0d81758d4c149f02b4068 Patch Third Party Advisory https://huntr.dev/bounties/3dab0466-c35d-4163-b3c7-a8666e2f7d95 Exploit Patch Third Party Advisory https://huntr.dev/bounties/3dab0466-c35d-4163-b3c7-a8666e2f7d95

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
Fortinet Releases Advisory on New Post-Exploitation Technique for Known Vulnerabilities	▪ Upgrade to FortiOS versions 7.6.2, 7.4.7, 7.2.11, 7.0.17, 6.4.16 to remove the malicious file and prevent re-compromise. ▪ Review the configuration of all in-scope devices. ▪ Reset potentially exposed credentials. ▪ As a work-around mitigation until the patch is applied, consider disabling SSL-VPN functionality, as exploitation of the file requires the SSL-VPN to be enabled.	https://www.cisa.gov/news-events/alerts/2025/04/11/fortinet-releases-advisory-new-post-exploitation-technique-known-vulnerabilities
Critical Vulnerabilitites in Microsoft Products	CVE-2025-29824, CVE-2025-26663, CVE-2025-26670, CVE-2025-27480, CVE-2025-27482, CVE-2025-29791, CVE-2025-27749, CVE-2025-27748, CVE-2025-27745, CVE-2025-27752	https://cow-prod-www-v3.azurewebsites.net/publications/security-advisories/2025-017/

News

Σύντομη περιγραφή / Τίτλος	URL
Cybercriminal groups embrace corporate structures to scale, sustain operations b	https://www.helpnetsecurity.com/2025/04/15/sandy-kronenberg-netarx-cybercriminal-groups-corporate-structures/
SSL/TLS certificate lifespans reduced to 47 days by 2029	https://www.bleepingcomputer.com/news/security/ssl-tls-certificate-lifespans-reduced-to-47-days-by-2029/
OpenAI's GPT-4.1, 4.1 nano, and 4.1 mini models release imminent	https://www.bleepingcomputer.com/news/artificial-intelligence/openais-gpt-41-41-nano-and-41-mini-models-release-imminent/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Govtech giant Conduent confirms client data stolen in January cyberattack	https://www.bleepingcomputer.com/news/security/govtech-giant-conduent-confirms-client-data-stolen-in-january-cyberattack/
Data Breach at Planned Parenthood Lab Partner Exposes Info of 1.6M	https://hackread.com/lab-breach-tied-planned-parenthood-compromises-records/
South African telecom provider Cell C disclosed a data breach following a cyberattack	https://securityaffairs.com/176509/data-breach/south-african-telecom-provider-cell-c-disclosed-a-data-breach.html
The quiet data breach hiding in AI workflows	https://www.helpnetsecurity.com/2025/04/14/quiet-data-breach-ai-workflows/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Gladinet flaw CVE-2025-30406 actively exploited in the wild	https://securityaffairs.com/176552/hacking/gladinet-flaw-cve-2025-30406-actively-exploited-in-the-wild.html
Major WordPress Plugin Flaw Exploited in Under 4 Hours	https://www.infosecurity-magazine.com/news/wordpress-plugin-flaw-exploited-4/
Rethinking Cyber Defense with Zero Trust + AI	https://thehackernews.com/expert-insights/2025/04/rethinking-cyber-defense-with-zero.html

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Fortinet Issues Fixes After Attackers Bypass Patches to Maintain Access	https://hackread.com/fortinet-fixe-attackers-bypass-patches-maintain-access/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Incomplete Patch Leaves NVIDIA and Docker Users at Risk	https://hackread.com/incomplete-patch-leaves-nvidia-docker-users-at-risk/
New malware 'ResolverRAT' targets healthcare, pharmaceutical firms	https://securityaffairs.com/176537/malware/new-malware-resolverrat-targets-healthcare-pharmaceutical-firms.html
Malicious NPM packages target PayPal users	https://securityaffairs.com/176530/security/malicious-npm-packages-to-steal-paypal-credentials.html

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Top 10 Best Cyber Attack Simulation Tools – 2025	https://cybersecuritynews.com/cyber-attack-simulation-tools/
Top Cybersecurity Tools of 2025 To Managing Remote Device Threats	https://cybersecuritynews.com/top-cybersecurity-tools-managing-remote-device-threats/

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/