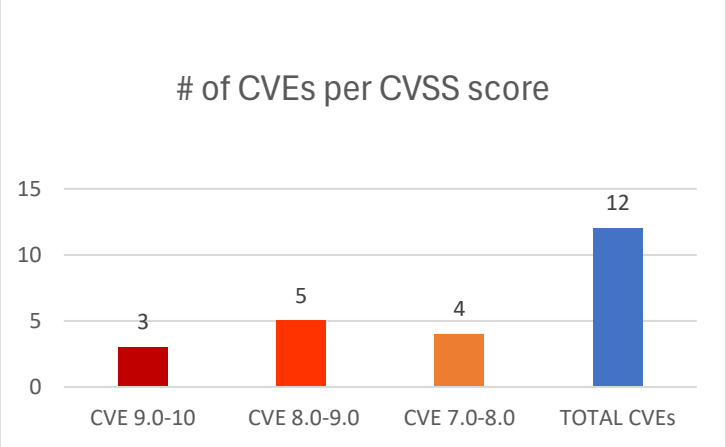
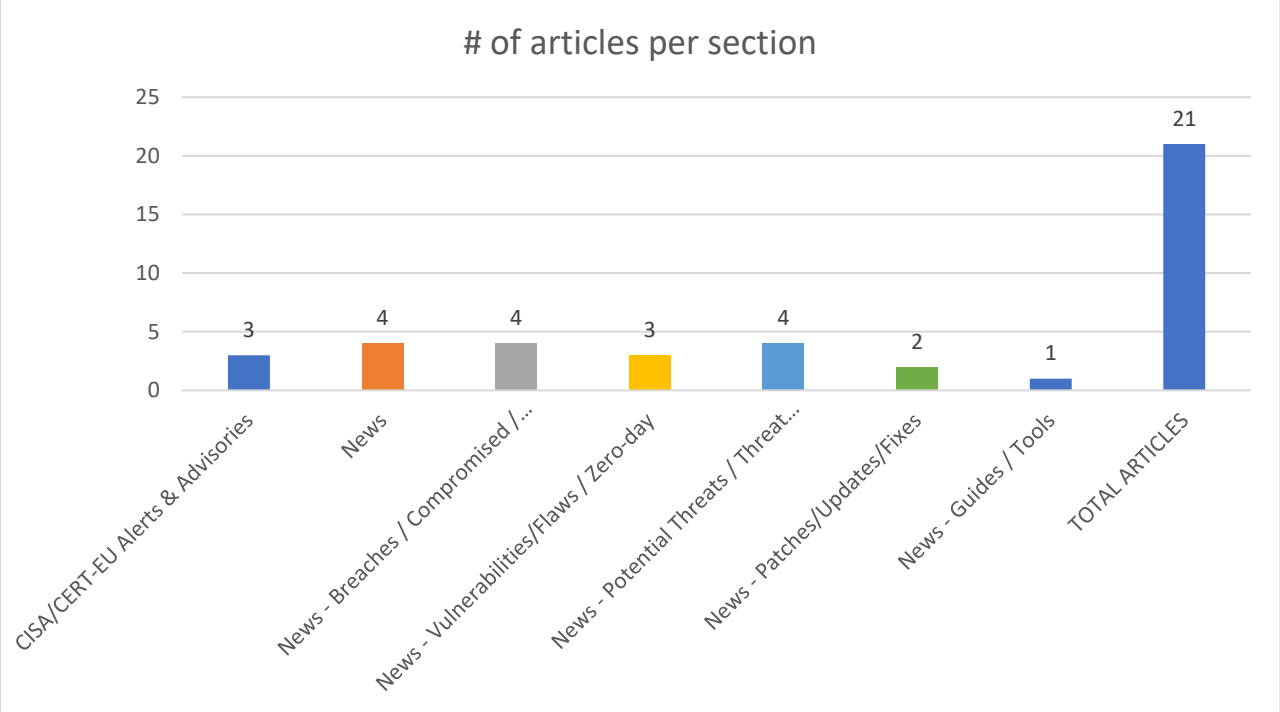
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 04/06/2025 - 06/06/2025





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-2025-5701	9,8	The HyperComments plugin for WordPress	Missing Authorization	all versions up to, and including, 1.2.2	https://plugins.trac.wordpress.org/browser/hypercomments/trunk/hypercomments.php https://www.wordfence.com/threat-intel/vulnerabilities/id/07fd6bee-5b00-4fc1-9f7a-3857fd35c763?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-5583	9,8	CodeAstro Real Estate Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://codeastro.com/ Product https://github.com/YZS17/CVE/blob/main/CodeAstro_Real_Estate_Management_System/sqli_register.php.md Exploit Third Party Advisory https://github.com/YZS17/CVE/blob/main/CodeAstro_Real_Estate_Management_System/sqli_register.php.md Exploit Third Party Advisory https://vuldb.com/?ctiid.311040 Permissions Required https://vuldb.com/?id.311040 Third Party Advisory VDB Entry https://vuldb.com/?submit.588822
https://nvd.nist.gov/vuln/detail/CVE-2025-5579	9,8	PHPGurukul Dairy Farm Shop Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.3	https://github.com/FLYFISH567/CVE/issues/14 Exploit Issue Tracking Third Party Advisory https://github.com/FLYFISH567/CVE/issues/14 Exploit Issue Tracking Third Party Advisory https://phpgurukul.com/ Product https://vuldb.com/?ctiid.311036 Permissions Required https://vuldb.com/?id.311036 Third Party Advisory VDB Entry https://vuldb.com/?submit.588804
https://nvd.nist.gov/vuln/detail/CVE-2025-5527	8,8	Tenda	Stack-based Buffer Overflow	RX3 16.03.13.11_multi_TDE01	https://github.com/alc9700jmo/CVE/issues/13 https://github.com/alc9700jmo/CVE/issues/13 https://vuldb.com/?ctiid.310967 https://vuldb.com/?id.310967 https://vuldb.com/?submit.586781 https://www.tenda.com.cn/

https://nvd.nist.gov/vuln/detail/CVE-2025-5671	8,8	TOTOLINK	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	N302R Plus up to 3.4.0-B20201028	https://github.com/byxs0x0/cve2/blob/main/530/1.md https://vuldb.com/?ctiid.311160 https://vuldb.com/?id.311160 https://vuldb.com/?submit.590093 https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2025-20261	8,8	Cisco Integrated Management Controller (IMC)	Improper Restriction of Communication Channel to Intended Endpoints	Cisco UCS B-Series, UCS C-Series, UCS S-Series, and UCS X-Series Servers	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-ssh-priv-esc-2mZDtdjM
https://nvd.nist.gov/vuln/detail/CVE-2025-5482	8,8	The Sunshine Photo Cart: Free Client Photo Galleries for Photographers plugin for WordPress	Unverified Password Change	all versions up to, and including, 3.4.11	https://plugins.trac.wordpress.org/browser/sunshine-photo-cart/trunk/includes/functions/account.php#L303 https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3305406%40sunshine-photo-cart%2Ftrunk&old=3261773%40sunshine-photo-cart%2Ftrunk&sfp_email=&sfph_mail= https://www.wordfence.com/threat-intel/vulnerabilities/id/5311b43c-14dd-4bdd-b6d0-d6468b831968?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-3055	8,1	The WP User Frontend Pro plugin for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	all versions up to, and including, 4.1.3	https://headwayapp.co/wp-user-frontend-changelog https://www.wordfence.com/threat-intel/vulnerabilities/id/eeb71c31-9e56-4b58-9cfc-a97f6892cc2b?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-5547	7,3	FreeFloat FTP Server	Improper Restriction of Operations within the Bounds of a Memory Buffer	1.0.	https://fitoxs.com/exploit/exploit-a9c9f7b4f50efc4b4be32e7ec4d3f7dfd7390e9be4ff168d9ab7a0eb911f8f3a1.txt https://vuldb.com/?ctiid.310997 https://vuldb.com/?id.310997 https://vuldb.com/?submit.586981

https://nvd.nist.gov/vuln/detail/CVE-2025-5634	7,3	PCMan FTP Server	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	2.0.7	https://fitoxs.com/exploit/exploit-c5e11f95f8d134e3c6b23c3b1b7ce5e79274ab0719f798f1bb509474b33b1c0e1.txt https://vuldb.com/?ctiid.311121 https://vuldb.com/?id.311121 https://vuldb.com/?submit.587048
https://nvd.nist.gov/vuln/detail/CVE-2025-5602	7,3	Campcodes Hospital Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/YZS17/CVE/blob/main/Hospital_Management_System/hms_admin_registration.php_sqli.md https://vuldb.com/?ctiid.311088 https://vuldb.com/?id.311088 https://vuldb.com/?submit.588842 https://www.campcodes.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-5562	7,3	PHPGurukul Curfew e-Pass Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/f1rstb100d/myCVE/issues/37 https://phpgurukul.com/ https://vuldb.com/?ctiid.311012 https://vuldb.com/?id.311012 https://vuldb.com/?submit.587544

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
Updated Guidance on Play Ransomware		**https://www.cisa.gov/news-events/alerts/2025/06/04/updated-guidance-play-ransomware**
CISA Releases Seven Industrial Control Systems Advisories	▪ **ICSA-25-155-01 CyberData 011209 SIP Emergency Intercom** ▪ **ICSA-25-155-02 Hitachi Energy Relion 670, 650 series and SAM600-IO Product** ▪ **ICSA-21-049-02 Mitsubishi Electric FA Engineering Software Products (Update H)** ▪ **ICSA-25-133-02 Hitachi Energy Relion 670/650/SAM600-IO Series (Update A)** ▪ **ICSA-23-068-05 Hitachi Energy Relion 670, 650 and SAM600-IO Series (Update A)** ▪ **ICSA-21-336-05 Hitachi Energy Relion 670/650/SAM600-IO (Update A)** ▪ **ICSA-23-089-01 Hitachi Energy IEC 61850 MMS-Server (Update A)**	https://www.cisa.gov/news-events/alerts/2025/06/05/cisa-releases-seven-industrial-control-systems-advisories
CISA Adds One Known Exploited Vulnerability to Catalog	▪ **CVE-2025-5419 Google Chromium V8 Out-of-Bounds Read and Write Vulnerability**	https://www.cisa.gov/news-events/alerts/2025/06/05/cisa-adds-one-known-exploited-vulnerability-catalog

News

Σύντομη περιγραφή / Τίτλος	URL
Microsoft unveils free EU cybersecurity program for governments	**https://www.bleepingcomputer.com/news/microsoft/microsoft-unveils-free-eu-cybersecurity-program-for-governments/**
Your SaaS Data Isn't Safe: Why Traditional DLP Solutions Fail in the Browser Era	https://thehackernews.com/2025/06/your-saas-data-isnt-safe-why.html
Ransomware and USB attacks are hammering OT systems	**https://www.helpnetsecurity.com/2025/06/06/honeywell-2025-cyber-threat-report/**
Germany fines Vodafone $51 million for privacy, security breaches	**https://www.bleepingcomputer.com/news/security/germany-fines-vodafone-51-million-for-privacy-security-breaches/**

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Exclusive: Hackers Leak 86 Million AT&T Records with Decrypted SSNs	**https://hackread.com/hackers-leak-86m-att-records-with-decrypted-ssns/**
Media giant Lee Enterprises says data breach affects 39,000 people	https://www.bleepingcomputer.com/news/security/media-giant-lee-enterprises-says-data-breach-affects-39-000-people/
Hacker arrested for breaching 5,000 hosting accounts to mine crypto	**https://www.bleepingcomputer.com/news/security/hacker-arrested-for-breaching-5-000-hosting-accounts-to-mine-crypto/**
Medical Data Breach Affected Dental Service Infrastructure	**https://dailysecurityreview.com/security-spotlight/medical-data-breach-affected-dental-service-infrastructure/**

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
CISA Issues Alert on Actively Exploited ScreenConnect, ASUS Router, and Craft CMS Vulnerabilities	**https://dailysecurityreview.com/security-spotlight/cisa-issues-alert-on-actively-exploited-screenconnect-asus-router-and-craft-cms-vulnerabilities/**
Critical Cisco ISE Auth Bypass Flaw Impacts Cloud Deployments on AWS, Azure, and OCI	https://thehackernews.com/2025/06/critical-cisco-ise-auth-bypass-flaw.html
HPE fixed multiple flaws in its StoreOnce software	https://securityaffairs.com/178629/security/hpe-fixed-multiple-flaws-in-its-storeonce-software.html

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
HPE fixed multiple flaws in its StoreOnce software	**https://securityaffairs.com/178629/security/hpe-fixed-multiple-flaws-in-its-storeonce-software.html**
Google fixes Chrome zero-day with in-the-wild exploit (CVE-2025-5419)	https://www.helpnetsecurity.com/2025/06/04/google-fixes-chrome-zero-day-with-in-the-wild-exploit-cve-2025-5419/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Malicious RubyGems Impersonate Fastlane Plugins to Steal Telegram Bot Data	**https://dailysecurityreview.com/security-spotlight/malicious-rubygems-impersonate-fastlane-plugins-to-steal-telegram-bot-data/**
New versions of Chaos RAT target Windows and Linux systems	https://securityaffairs.com/178670/malware/new-versions-of-chaos-rat-target-windows-and-linux-systems.html
#Infosec2025: DNS Hijacking, A Major Cyber Threat for the UK Government	https://www.infosecurity-magazine.com/news/infosec2025-dns-hijacking-uk/
Google: Hackers target Salesforce accounts in data extortion attacks	**https://www.bleepingcomputer.com/news/security/google-hackers-target-salesforce-accounts-in-data-extortion-attacks/**

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Top Tools for Enterprise Security Monitoring	https://cybersecuritynews.com/enterprise-security-monitoring-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.

[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/