Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 07/03/2025 - 11/03/2025

Contents

1 Common Vulnerabilities and Exposures (CVEs)

URL ευπάθειας (NIST NVD)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	Συσκευές/Εκδόσεις που ΔΕΝ επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2025-27816	9.8	Arctera InfoScale	Deserialization of Untrusted Data	7.0 through 8.0.2	N/A	https://www.arctera.io/infoscale https://www.veritas.com/content/support/en_US/security/ARC25-002
https://nvd.nist.gov/vuln/detail/CVE-2025-1661	9.8	HUSKY – Products Filter Professional for WooCommerce plugin for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	all versions up to, and including, 1.3.6.5	N/A	https://el.wordpress.org/plugins/woocommerce-products-filter/ https://www.wordfence.com/threat-intel/vulnerabilities/id/9ae7b6fc-2120-4573-8b1b-d5422d435fa5?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-56336	9.8	SINAMICS S200	Improper Authentication	All versions with serial number beginning with SZVS8, SZVS9, SZVS0 or SZVSN and the FS number is 02	N/A	https://www.siemens.com/global/en/products/drives/sinamics/low-voltage-converters/servo-converter/sinamics-s200.html https://cert-portal.siemens.com/productcert/html/ssa-787280.html
https://nvd.nist.gov/vuln/detail/CVE-2025-27494	9.1	SiPass integrated	Improper Input Validation	AC5102 (ACC-G2) (All versions < V6.4.9), SiPass integrated ACC-AP (All versions < V6.4.9)	N/A	https://shop.vanderbiltindustries.com/uk-en/access-control/systems/sipass-integrated/controllers/657/ac5102-advanced-central-controller https://cert-portal.siemens.com/productcert/html/ssa-515903.html
https://nvd.nist.gov/vuln/detail/CVE-2025-2097	8.8	TOTOLINK EX1800T	Improper Restriction of Operations within the Bounds of a Memory Buffer	.1.0cu.2112_B20220316	N/A	https://www.totolink.net/home/menu/newstpl/menu_newstpl/products/id/223.html https://github.com/kn0sky/cve/blob/main/TOTOLINK%20EX1800T/Stack-based%20Buffer%20Overflow%2001%20setRptWizardCfg-_loginpass.md
https://nvd.nist.gov/vuln/detail/CVE-2025-27912	8.8	Datalust Seq	Cross-Site Request Forgery (CSRF)	before 2024.3.13545	N/A	https://datalust.co/seq https://datalust.co/seq https://github.com/datalust/seq-tickets/issues/2366
https://nvd.nist.gov/vuln/detail/CVE-2025-27434	8.8	SAP Commerce	Cross-site Scripting	N/A	N/A	https://www.sap.com/products/crm/commerce-cloud.html https://me.sap.com/notes/3569602 https://url.sap/sapsecuritypatchday
https://nvd.nist.gov/vuln/detail/CVE-2025-26661	8.8	SAP NetWeaver (ABAP Class Builder)	Missing Authorization	N/A	N/A	https://en.wikipedia.org/wiki/SAP_NetWeaver https://me.sap.com/notes/3563927 https://url.sap/sapsecuritypatchday
https://nvd.nist.gov/vuln/detail/CVE-2025-1920	8.8	Google Chrome	Access of Resource Using Incompatible Type ('Type Confusion')	prior to 134.0.6998.88	N/A	https://www.google.com/chrome/ https://chromereleases.googleblog.com/2025/03/stable-channel-update-for-desktop_10.html https://issues.chromium.org/issues/398065918
https://nvd.nist.gov/vuln/detail/CVE-2025-27396	8.8	SCALANCE LPE9403	Improper Check for Dropped Privileges	6GK5998-3GS00-2AC2) (All versions < V4.0	N/A	https://mall.industry.siemens.com/mall/zh/WW/Catalog/Products/10399441 https://cert-portal.siemens.com/productcert/html/ssa-075201.html

https://nvd.nist.gov/vuln/detail/CVE-2024-41724	8.7	Gallagher Command Centre SALTO	Improper Certificate Validation	prior to 9.20.1043	N/A	https://products.security.gallagher.com/security/global/en/products/integrations/salto-wireless-access-integration/p/BVINT167 https://security.gallagher.com/en-NZ/Security-Advisories/CVE-2024-41724
https://nvd.nist.gov/vuln/detail/CVE-2025-27925	8.5	Nintex Automation	Deserialization of Untrusted Data	5.6 and 5.7 before 5.8	N/A	https://www.nintex.com/ https://help.nintex.com/en-US/platform/ReleaseNotes/K2Five.htm
https://nvd.nist.gov/vuln/detail/CVE-2024-56182	8.2	SIMATIC products	Protection Mechanism Failure	Multiple versions/products	N/A	https://assets.new.siemens.com/siemens/assets/api/uuid:725039f7-1270-43aa-9dc7-54a5d739b594/dffa-b10336-00-7600.pdf https://cert-portal.siemens.com/productcert/html/ssa-216014.html
https://nvd.nist.gov/vuln/detail/CVE-2024-13359	8.1	Product Input Fields for WooCommerce plugin for WordPress	Unrestricted Upload of File with Dangerous Type	all versions up to, and including, 1.12.1	N/A	https://wordpress.org/plugins/product-input-fields-for-woocommerce/ https://www.wordfence.com/threat-intel/vulnerabilities/id/a9c08f2e-bffd-40a6-89f3-559cb34f4395?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-26331	7.8	Dell ThinOS	Command Injection	2411 and prior	N/A	https://www.dell.com/en-us/lp/dell-thinos https://www.dell.com/support/kbdoc/en-us/000289886/dsa-2025-107
https://nvd.nist.gov/vuln/detail/CVE-2022-43454	7.8	Apple products	Double Free	N/A	macOS Ventura 13.1, watchOS 9.2, iOS 16.2 and iPadOS 16.2, tvOS 16.2	https://www.apple.com/gr/ https://support.apple.com/en-us/102741 https://support.apple.com/en-us/102807 https://support.apple.com/en-us/102808 https://support.apple.com/en-us/102836
https://nvd.nist.gov/vuln/detail/CVE-2025-27438	7.8	Teamcenter Visualization & Tecnomatix Plant Simulation	Out-of-bounds Read	Multiple versions/products	N/A	https://plm.sw.siemens.com/en-US/teamcenter/solutions/product-visualization-digital-mockup-software/ https://cert-portal.siemens.com/productcert/html/ssa-050438.html
https://nvd.nist.gov/vuln/detail/CVE-2024-13908	7.2	SMTP by BestWebSoft plugin for WordPress	Unrestricted Upload of File with Dangerous Type	all versions up to, and including, 1.1.9	N/A	https://wordpress.org/plugins/bws-smtp/ https://www.wordfence.com/threat-intel/vulnerabilities/id/9f3b0637-b1ee-4e0b-95cd-11ac377805a7?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-12009	7.2	Zyxel EX5601-T1	OS Command Injection	V5.70(ACDZ.3.6)C0 and earlier	N/A	https://www.zyxel.com/service-provider/global/en/products/ethernet-cpe/ethernet-iads/ex5601ex5600-t-series https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-post-authentication-command-injection-vulnerabilities-in-certain-dsl-ethernet-cpe-fiber-ont-and-wifi-extender-devices-03-11-2025
https://nvd.nist.gov/vuln/detail/CVE-2024-11253	7.2	Zyxel VMG8825-T50K	OS Command Injection	V5.50(ABOM.8.5)C0 and earlier	N/A	https://www.zyxel.com/global/en/products/dsl-cpe/dual-band-wireless-ac-n-vdsl2-combo-wan-gigabit-iad-vmg8825-t50k https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-post-authentication-command-injection-vulnerabilities-in-certain-dsl-ethernet-cpe-fiber-ont-and-wifi-extender-devices-03-11-2025
https://nvd.nist.gov/vuln/detail/CVE-2024-12010	7.2	Zyxel AX7501-B1	OS Command Injection	V5.17(ABPC.5.3)C0 and earlier	N/A	https://www.zyxel.com/service-provider/global/en/products/fiber-oltsonts/10g-active-fiber/hgus/ax7501-b1 https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-post-authentication-command-injection-

						vulnerabilities-in-certain-dsl-ethernet-cpe-fiber-ont-and-wifi-extender-devices-03-11-2025
https://nvd.nist.gov/vuln/detail/CVE-2025-0162	7.1	IBM Aspera Shares	Improper Restriction of XML External Entity Reference	1.9.9 through 1.10.0 PL7	N/A	https://www.ibm.com/docs/en/aspera-connect/4.0?topic=windows-working-aspera-shares https://www.ibm.com/support/pages/node/7185096
https://nvd.nist.gov/vuln/detail/CVE-2024-53693	7.1	QNAP operating system	Improper Neutralization of CRLF Sequences ('CRLF Injection')	N/A	QTS 5.2.3.3006 build 20250108 and later QuTS hero h5.2.3.3006 build 20250108 and later	https://www.qnap.com/en/operating-system/qts https://www.qnap.com/en/security-advisory/qsa-24-54

2 CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
Vulnerability Summary for the Week of February 24, 2025	Common Vulnerabilities and Exposures (CVE)	https://www.cisa.gov/news-events/bulletins/sb25-062
CISA Adds Five Known Exploited Vulnerabilities to Catalog	CVE-2025-25181 Advantive VeraCore SQL Injection Vulnerability CVE-2024-57968 Advantive VeraCore Unrestricted File Upload Vulnerability CVE-2024-13159 Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability CVE-2024-13160 Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability CVE-2024-13161 Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability	https://www.cisa.gov/news-events/alerts/2025/03/10/cisa-adds-five-known-exploited-vulnerabilities-catalog

3 News

Σύντομη περιγραφή / Τίτλος	URL
March 2025 Patch Tuesday forecast: A return to normalcy	https://www.helpnetsecurity.com/2025/03/10/march-2025-patch-tuesday-forecast/
SECURITY AFFAIRS MALWARE NEWSLETTER ROUND 36	https://securityaffairs.com/175124/malware/security-affairs-malware-newsletter-round-36.html
Quantum leap: Passwords in the new era of computing security	https://www.bleepingcomputer.com/news/security/quantum-leap-passwords-in-the-new-era-of-computing-security/
Swiss critical sector faces new 24-hour cyberattack reporting rule	https://www.bleepingcomputer.com/news/security/swiss-critical-sector-faces-new-24-hour-cyberattack-reporting-rule/
US govt says Americans lost record $12.5 billion to fraud in 2024	https://www.bleepingcomputer.com/news/security/us-govt-says-americans-lost-record-125-billion-to-fraud-in-2024/
DDoS Blamed as X Suffers Multiple Outages	https://www.infosecurity-magazine.com/news/ddos-blamed-x-suffers-multiple/

3.1 Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Data breach at Japanese telecom giant NTT hits 18,000 companies	https://www.bleepingcomputer.com/news/security/data-breach-at-japanese-telecom-giant-ntt-hits-18-000-companies/
Bank of America Issues Warning on Data Breach: Millions of Accounts at Risk	https://dailysecurityreview.com/security-spotlight/bank-of-america-issues-warning-on-data-breach-millions-of-accounts-at-risk/

3.2 Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Apache Traffic Server Vulnerabilities Let Attackers Perform Malformed Requests	https://cybersecuritynews.com/apache-traffic-server-vulnerabilities/
Popular Python Library Vulnerability Exposes 43 million Installations to Code Execution Attacks	https://cybersecuritynews.com/popular-python-library-vulnerability/
Experts warn of mass exploitation of critical PHP flaw CVE-2024-4577	https://securityaffairs.com/175198/hacking/experts-warn-of-mass-exploitation-of-critical-php-flaw-cve-2024-4577.html
Critical Veritas Vulnerability Let Attackers Execute Malicious Code	https://cybersecuritynews.com/critical-veritas-vulnerability/
Apache Tomcat Vulnerability Exposes Servers to RCE Attacks	https://cybersecuritynews.com/apache-tomcat-vulnerability-rce-attacks/

3.3 Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Chrome Security Update – Patch for Multiple High-Severity Vulnerabilities	https://cybersecuritynews.com/patch-for-multiple-high-severity-vulnerabilities/
Moxa Issues Fix for Critical Authentication Bypass Vulnerability in PT Switches	https://thehackernews.com/2025/03/moxa-issues-fix-for-critical.html

3.4 Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
1 Million Devices Infected by Malwares Hosted on GitHub, Microsoft Warns	https://cybersecuritynews.com/1-million-devices-infected-by-malwares-hosted-on-github/
Commvault Webserver Vulnerability Let Attackers Compromise Webserver	https://cybersecuritynews.com/commvault-webserver-vulnerability/
Medusa Ransomware targeted over 40 organizations in 2025	https://securityaffairs.com/175013/malware/medusa-ransomware-targeted-over-40-organizations-in-2025.html
12,000 API Keys and Passwords Found in AI Training Datasets	https://dailysecurityreview.com/security-spotlight/12000-api-keys-and-passwords-found-in-ai-training-datasets/
Unpatched Edimax IP camera flaw actively exploited in botnet attacks	https://www.bleepingcomputer.com/news/security/unpatched-edimax-ip-camera-flaw-actively-exploited-in-botnet-attacks/
Lazarus Hackers Weaponized 6 npm Packages To Steal Logins	https://cybersecuritynews.com/lazarus-hackers-weaponized-6-npm-packages/
5000+ Malicious Packages Found In The Wild To Compromise Windows Systems	https://cybersecuritynews.com/5000-malicious-packages-found-in-the-wild/
Over 1000 Malicious Packages Found Exploiting Open-Source Platforms	https://hackread.com/malicious-packages-exploiting-open-source-platforms/
SideWinder APT targets maritime and nuclear sectors with enhanced toolset	https://securityaffairs.com/175247/apt/sidewinder-apt-targets-maritime-nuclear-sectors.html
EncryptHub A Multi-Stage Malware Compromised 600 Organizations	https://cybersecuritynews.com/encrypthub-a-multi-stage-malware/
Threat Actor Allegedly Selling Bruteforcer for Cisco VPN	https://cybersecuritynews.com/bruteforcer-for-cisco-vpn/

3.5 Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Hetty: Open-source HTTP toolkit for security research	https://www.helpnetsecurity.com/2025/03/10/hetty-open-source-http-toolkit-security-research/
How to safely dispose of old tech without leaving a security risk	https://www.helpnetsecurity.com/2025/03/10/old-tech-dispose-security-risk/
Microsoft shares guidance on upcoming Publisher deprecation	https://www.bleepingcomputer.com/news/microsoft/microsoft-shares-guidance-on-upcoming-publisher-deprecation/
Top 11 Passwordless Authentication Tools – 2025	https://cybersecuritynews.com/passwordless-authentication/

4 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.

5 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/