Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 18/03/2025 - 21/03/2025

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-2025-29783	**10**	vLLM	Deserialization of Untrusted Data	N/A	https://github.com/vllm-project/vllm/commit/288ca110f68d23909728627d3100e5a8db820aa2 https://github.com/vllm-project/vllm/pull/14228 https://github.com/vllm-project/vllm/security/advisories/GHSA-x3m8-f7g5-qhm7
https://nvd.nist.gov/vuln/detail/CVE-2024-10442	**10**	Synology Replication Service	Off-by-one Error	before 1.0.12-0066, 1.2.2-0353 and 1.3.0-0423 and Synology Unified Controller (DSMUC) before 3.1.4-23079	https://www.synology.com/en-global/security/advisory/Synology_SA_24_22
https://nvd.nist.gov/vuln/detail/CVE-2024-56346	**10**	IBM AIX 7.2 and 7.3 nimesis NIM master service could	Process Control	IBM AIX 7.2 and 7.3 nimesis NIM master service could	https://www.ibm.com/support/pages/node/7186621
https://nvd.nist.gov/vuln/detail/CVE-2025-29137	**9,8**	Tenda AC7	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	Tenda AC7 V1.0 V15.03.06.44	https://github.com/Raining-101/IOT_cve/blob/main/tenda-ac7form_fast_setting_wifi_set%20timeZone.md
https://nvd.nist.gov/vuln/detail/CVE-2025-2512	**9,8**	File Away plugin for WordPress	Unrestricted Upload of File with Dangerous Type	all versions up to, and including, 3.9.9.0.1	https://plugins.trac.wordpress.org/browser/file-away/trunk/lib/cls/class.fileaway_management.php#L1094 https://wordpress.org/plugins/file-away/#developers https://www.wordfence.com/threat-intel/vulnerabilities/id/9a93313d-a5d7-4109-93c5-b2da26e7a486?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-10441	**9,8**	Synology BeeStation Manager	Improper Encoding or Escaping of Output	Synology BeeStation Manager (BSM) before 1.1-65374	https://www.synology.com/en-global/security/advisory/Synology_SA_24_20 https://www.synology.com/en-global/security/advisory/Synology_SA_24_23

				and Synology DiskStation Manager (DSM) before 7.2-64570-4, 7.2.1-69057-6 and 7.2.2-72806-1	
https://nvd.nist.gov/vuln/detail/CVE-2023-47539	**9,8**	FortiMail	Improper Access Control	FortiMail version 7.4.0	https://fortiguard.com/psirt/FG-IR-23-439
https://nvd.nist.gov/vuln/detail/CVE-2024-7804	**9,8**	Pytorch RPC framework	Deserialization of Untrusted Data	versions <=2.3.1	https://huntr.com/bounties/0e870eeb-f924-4054-8fac-d926b1fb7259
https://nvd.nist.gov/vuln/detail/CVE-2025-1770	**8,8**	Event Manager, Events Calendar, Tickets, Registrations – Eventin plugin for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	all versions up to, and including, 4.0.24 via the 'style' parameter	https://plugins.trac.wordpress.org/browser/wp-event-solution/tags/4.0.24/widgets/events-calendar/events-calendar.php#L715 https://plugins.trac.wordpress.org/browser/wp-event-solution/tags/4.0.24/widgets/upcoming-event-tab/style/tab-1.php#L53 https://plugins.trac.wordpress.org/changeset/3257023/ https://www.wordfence.com/threat-intel/vulnerabilities/id/5f24baee-7003-449b-9072-d95fa1e26c8f?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-30236	**8,6**	Shearwater SecurEnvoy SecurAccess	External Control of Assumed-Immutable Web Parameter	before 9.4.515	https://reserge.org/probabilistically-breaking-securenvoy-totp/ https://securenvoy.com/wp-content/uploads/2025/03/Release-Notes-9.4.515.pdf
https://nvd.nist.gov/vuln/detail/CVE-2024-51459	**8,4**	IBM InfoSphere Information Server 11.7 could	Improper Handling of Insufficient Permissions or Privileges	11.7	https://www.ibm.com/support/pages/node/7185056
https://nvd.nist.gov/vuln/detail/CVE-2024-21760	**8,4**	FortiSOAR Connector	Improper Control of Generation of Code ('Code Injection')	FortiSOAR Connector FortiSOAR 7.4 all versions, 7.3 all versions, 7.2 all versions, 7.0 all versions, 6.4 all versions	https://fortiguard.fortinet.com/psirt/FG-IR-23-420
https://nvd.nist.gov/vuln/detail/CVE-2025-0755	**8,4**	MongoDB	Heap-based Buffer Overflow	MongoDB C driver library	https://jira.mongodb.org/browse/SERVER-94461

https://nvd.nist.gov/vuln/detail/CVE-2025-27688	**7,8**	Dell ThinOS 2408	Incorrect Permission Assignment for Critical Resource	Dell ThinOS 2408 and prior	https://www.dell.com/support/kbdoc/en-us/000289886/dsa-2025-107
https://nvd.nist.gov/vuln/detail/CVE-2025-27415	**7,5**	Nuxt	Acceptance of Extraneous Untrusted Data With Trusted Data	Prior to 3.16.0	https://github.com/nuxt/nuxt/security/advisories/GHSA-jvhm-gjrh-3h93
https://nvd.nist.gov/vuln/detail/CVE-2024-50631	**7,5**	Synology Drive Server	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Synology Drive Server before 3.0.4-12699, 3.2.1-23280, 3.5.0-26085 and 3.5.1-26102	https://www.synology.com/en-global/security/advisory/Synology_SA_24_21

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds Three Known Exploited Vulnerabilities to Catalog	**CVE-2025-1316 Edimax IC-7100 IP Camera OS Command Injection Vulnerability** **CVE-2024-48248 NAKIVO Backup and Replication Absolute Path Traversal Vulnerability** **CVE-2017-12637 SAP NetWeaver Directory Traversal Vulnerability**	**https://www.cisa.gov/news-events/alerts/2025/03/19/cisa-adds-three-known-exploited-vulnerabilities-catalog**
Supply Chain Compromise of Third-Party GitHub Action, CVE-2025-30066	**CVE-2025-30066**	**https://www.cisa.gov/news-events/alerts/2025/03/18/supply-chain-compromise-third-party-github-action-cve-2025-30066**
CISA Adds Two Known Exploited Vulnerabilities to Catalog	**CVE-2025-24472 Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability** **CVE-2025-30066 tj-actions/changed-files GitHub Action Embedded Malicious Code Vulnerability**	**https://www.cisa.gov/news-events/alerts/2025/03/18/cisa-adds-two-known-exploited-vulnerabilities-catalog**
CISA Releases Seven Industrial Control Systems Advisories	**ICSA-25-077-01 Schneider Electric EcoStruxure Power Automation System User Interface (EPAS-UI)** **ICSA-25-077-02 Rockwell Automation Lifecycle Services with VMware** **ICSA-25-077-03 Schneider Electric EcoStruxure Power Automation System** **ICSA-25-077-04 Schneider Electric EcoStruxure Panel Server** **ICSA-25-077-05 Schneider Electric ASCO 5310/5350 Remote Annunciator** **ICSA-24-352-04 Schneider Electric Modicon (Update A)** **ICSA-24-291-03 Mitsubishi Electric CNC Series (Update B)**	**https://www.cisa.gov/news-events/alerts/2025/03/18/cisa-releases-seven-industrial-control-systems-advisories**
Rockwell Automation Lifecycle Services with VMware	**CVE-2025-22224**	**https://www.cisa.gov/news-events/ics-advisories/icsa-25-077-02**
CISA Releases Five Industrial Control Systems Advisories	ICSA-25-079-01 Schneider Electric EcoStruxure™ ICSA-25-079-02 Schneider Electric Enerlin'X IFE and eIFE ICSA-25-079-03 Siemens Simcenter Femap ICSA-25-079-04 SMA Sunny Portal ICSMA-25-079-01 Santesoft Sante DICOM Viewer Pro	https://www.cisa.gov/news-events/alerts/2025/03/20/cisa-releases-five-industrial-control-systems-advisories

News

Σύντομη περιγραφή / Τίτλος	URL
Bypassing OTP Verification: Another Bug Found Without Any Tools!	https://strangerwhite.medium.com/bypassing-otp-verification-another-bug-found-without-any-tools-8b2c1013c3e7
Understanding Types of Cyberattacks	https://medium.com/@cyberlois/understanding-types-of-cyberattacks-9f7c216d4a89
Cloud Security Governance	https://medium.com/@cyberlois/cloud-security-governance-46ab58aea085
Kali Linux 2025.1a Released With New Tool & Updates to Desktop Environments	https://cybersecuritynews.com/kali-linux-2025-1a/
Hackers Leveraging RMM Tools To Maintain Persistence To Infiltrate And Move Through Networks	https://cybersecuritynews.com/hackers-leveraging-rmm-tools/
Threat Actors Exploiting Legacy Drivers to Bypass TLS Certificate Validation	https://cybersecuritynews.com/threat-actors-exploiting-legacy-drivers/
Attackers Embedding Malicious Word file into a PDF to Evade Detections	https://cybersecuritynews.com/attackers-embedding-malicious-word-file-into-a-pdf/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
US Sperm Donor Giant California Cryobank Hacked – Customers Personal Data Exposed	https://cybersecuritynews.com/us-sperm-donor-giant-california-cryobank-hackers/
41% of Success Logins Across Websites Involves Compromised Passwords	https://cybersecuritynews.com/41-of-success-logins-across-websites/
Arcane Stealer Via YouTube Videos Steal Data From Network Utilities Including VPN & FileZilla	https://cybersecuritynews.com/arcane-stealer-via-youtube-videos/
Threat Actors Stolen Over 3.2 Billion Login Credentials & Infected 23 Million Devices Worldwide	https://cybersecuritynews.com/threat-actors-stolen-over-3-2-billion-login-credentials/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Threat Actors Exploiting Chrome DLL Side-Loading Vulnerability to Execute Malware	https://cybersecuritynews.com/threat-actors-exploiting-dll-side-loading-vulnerability/
PHP RCE Vulnerability Actively Exploited in Wild to Attack Windows-based Systems	https://cybersecuritynews.com/php-rce-vulnerability-actively-exploited-in-wild/
Critical Synology Vulnerability Let Attackers Remote Execute Arbitrary Code	https://cybersecuritynews.com/synologys-diskstation-manager-vulnerability/
8-Year Old Windows Shortcut Zero-Day Exploited by 11 State-Sponsored Hacker Groups	https://cybersecuritynews.com/8-year-old-windows-shortcut-zero-day/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
CISA Warns of Supply-Chain Attack Targeting Widely-Used GitHub Action Vulnerability	https://cybersecuritynews.com/cisa-warns-of-supply-chain-attack/
Microsoft to End Support for Windows 10, No More Security Updates!	https://cybersecuritynews.com/microsoft-to-end-support-for-windows-10/
Sophisticated Attack Via Booking Websites Installs LummaStealer Malware	https://cybersecuritynews.com/attack-via-booking-websites-installs-lummastealer/
Beware of Fake Coinbase Migration Messages Aimed to Steal Your Wallet Credentials	https://cybersecuritynews.com/beware-of-fake-coinbase-migration-messages/
CISA Warns of Fortinet FortiOS Authentication Bypass Vulnerability Exploited in Wild	https://cybersecuritynews.com/cisa-fortinet-fortios-authentication/
Microsoft Warns of New StilachiRAT Stealing Remote Desktop Protocol Sessions Data	https://cybersecuritynews.com/microsoft-warns-of-new-stilachirat/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Caido v0.47.0 Released – Burp Suite Alternative Web Pentesting Tool Brings New Features	https://cybersecuritynews.com/caido-v0-47-0-released/

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/