Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 15/04/2025 - 17/04/2025

Contents

Common Vulnerabilities and Exposures (CVEs)

URL ευπάθειας (NIST NVD)	CVSSv4	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2021-27460	**10**	Rockwellautomation	.NET remoting endpoints that deserialize untrusted data	Rockwell Automation FactoryTalk AssetCentre v10.00 and earlier	https://idp.rockwellautomation.com/adfs/ls/idpinitiatedsignon.aspx?RelayState=RPID%3Drockwellautomation.custhelp.com%26RelayState%3Danswers%2Fanswer_view%2Fa_id%2F1130831 Permissions Required Vendor Advisory https://idp.rockwellautomation.com/adfs/ls/idpinitiatedsignon.aspx?RelayState=RPID%3Drockwellautomation.custhelp.com%26RelayState%3Danswers%2Fanswer_view%2Fa_id%2F1130831 Permissions Required Vendor Advisory https://www.cisa.gov/uscert/ics/advisories/icsa-21-091-01 Third Party Advisory US Government Resource https://www.cisa.gov/uscert/ics/advisories/icsa-21-091-01
https://nvd.nist.gov/vuln/detail/CVE-2022-46326	**9,8**	Huawei	out-of-bounds write vulnerability	Emui Harmonyos	https://consumer.huawei.com/en/support/bulletin/2022/12/ Patch Vendor Advisory https://consumer.huawei.com/en/support/bulletin/2022/12/ Patch Vendor Advisory https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397 Patch Vendor Advisory https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397

https://nvd.nist.gov/vuln/detail/CVE-2024-33444	**9,8**	Onethink	SQL injection	onethink v.1.1	https://gist.github.com/LioTree/1971a489dd5ff619b89e7a9e1da91152
https://nvd.nist.gov/vuln/detail/CVE-2022-47629	**9,8**	Debian, Gnupg, Redhat	Debian Linux, Libksba, Enterprise Linux Jbosseapxp Rhel Aus Rhel E4s Rhel Eus Rhel Tus Rhev Hypervisor	Libksba before 1.6.3	https://dev.gnupg.org/T6284 Patch Third Party Advisory https://dev.gnupg.org/T6284 Patch Third Party Advisory https://git.gnupg.org/cgi-bin/gitweb.cgi?p=libksba.git%3Ba=commit%3Bh=f61a5ea4e0f6a80fd4b28ef0174bee77793cf070 https://git.gnupg.org/cgi-bin/gitweb.cgi?p=libksba.git%3Ba=commit%3Bh=f61a5ea4e0f6a80fd4b28ef0174bee77793cf070 https://lists.debian.org/debian-lts-announce/2022/12/msg00035.html Mailing List Third Party Advisory https://lists.debian.org/debian-lts-announce/2022/12/msg00035.html Mailing List Third Party Advisory https://security.gentoo.org/glsa/202212-07 Third Party Advisory https://security.gentoo.org/glsa/202212-07 Third Party Advisory https://security.netapp.com/advisory/ntap-20230316-0011/ https://security.netapp.com/advisory/ntap-20230316-0011/ https://www.debian.org/security/2022/dsa-5305 Third Party Advisory https://www.debian.org/security/2022/dsa-5305
https://nvd.nist.gov/vuln/detail/CVE-2022-46421	**9,8**	Apache	Improper Neutralization	Apache Airflow Hive Provider: before 5.0.0	https://github.com/apache/airflow/pull/28101 Patch Third Party Advisory https://github.com/apache/airflow/pull/28101 Patch Third Party Advisory https://lists.apache.org/thread/09twdoyoybldlfj5gvk0qswtofh0rmp4 Mailing List Patch Vendor Advisory https://lists.apache.org/thread/09twdoyoybldlfj5gvk0qswtofh0rmp4

https://nvd.nist.gov/vuln/detail/CVE-2022-26069	**9,8**	Delta Electronics DIAEnergie	SQL injection	All versions prior to 1.8.02.004	https://www.cisa.gov/uscert/ics/advisories/icsa-22-081-01 Mitigation Third Party Advisory US Government Resource https://www.cisa.gov/uscert/ics/advisories/icsa-22-081-01
https://nvd.nist.gov/vuln/detail/CVE-2021-4129	**9,8**	Mozilla	memory corruption	Firefox < 95, Firefox ESR < 91.4.0, and Thunderbird < 91.4.0	https://bugzilla.mozilla.org/buglist.cgi?bug_id=1393362%2C1736046%2C1736751%2C1737009%2C1739372%2C1739421 Exploit Issue Tracking Vendor Advisory https://bugzilla.mozilla.org/buglist.cgi?bug_id=1393362%2C1736046%2C1736751%2C1737009%2C1739372%2C1739421 Exploit Issue Tracking Vendor Advisory https://www.mozilla.org/security/advisories/mfsa2021-52/ Vendor Advisory https://www.mozilla.org/security/advisories/mfsa2021-52/ Vendor Advisory https://www.mozilla.org/security/advisories/mfsa2021-53/ Vendor Advisory https://www.mozilla.org/security/advisories/mfsa2021-53/ Vendor Advisory https://www.mozilla.org/security/advisories/mfsa2021-54/ Vendor Advisory https://www.mozilla.org/security/advisories/mfsa2021-54/

https://nvd.nist.gov/vuln/detail/CVE-2021-38395	**9,8**	Honeywell	improper neutralization	Honeywell Experion PKS C200, C200E, C300, and ACE controllers	https://www.cisa.gov/uscert/ics/advisories/icsa-21-278-04 Mitigation Third Party Advisory US Government Resource https://www.cisa.gov/uscert/ics/advisories/icsa-21-278-04 Mitigation Third Party Advisory US Government Resource https://www.honeywellprocess.com/library/support/notifications/Customer/SN2021-02-22-01-Experion-C300-CCL.pdf Product https://www.honeywellprocess.com/library/support/notifications/Customer/SN2021-02-22-01-Experion-C300-CCL.pdf
https://nvd.nist.gov/vuln/detail/CVE-2023-41503	**9,8**	Php	Improper Control of Generation of Code ('Code Injection')	PHP v1.0	https://github.com/ASR511-OO7/CVE-2023-41503/blob/main/CVE-26 https://github.com/ASR511-OO7/CVE-2023-41503/blob/main/CVE-26
https://nvd.nist.gov/vuln/detail/CVE-2025-27674	**9,8**	Printerlogic	Use of Hard-coded Cryptographic Key	Vasion Print (formerly PrinterLogic) before Virtual Appliance Host 22.0.843 Application 20.0.1923	https://help.printerlogic.com/saas/Print/Security/Security-Bulletins.htm Vendor Advisory https://pierrekim.github.io/blog/2025-04-08-vasion-printerlogic-83-vulnerabilities.html

https://nvd.nist.gov/vuln/detail/CVE-2024-57225	**9,8**	Linksys	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Linksys E7350 1.1.00.032	https://github.com/yanggao017/vuln/blob/main/Linksys/E7350/CI_7_reset_wifi/README.md
https://nvd.nist.gov/vuln/detail/CVE-2025-21613	**9,8**	go-git	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	versions prior to v5.13	https://github.com/go-git/go-git/security/advisories/GHSA-v725-9546-7q7m
https://nvd.nist.gov/vuln/detail/CVE-2024-11613	**9,8**	The WordPress File Upload plugin for WordPress	Improper Control of Generation of Code ('Code Injection')	all versions up to, and including, 4.24.15	https://plugins.svn.wordpress.org/wp-file-upload/trunk/wfu_file_downloader.php Product https://plugins.trac.wordpress.org/changeset/3217005/ Patch https://www.wordfence.com/threat-intel/vulnerabilities/id/31052fe6-a0ae-4502-b2d2-dbc3b3bf672f?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-25509	**9,4**	Ruvar	SQL injection	RuvarOA v6.01 and v12.01	https://gist.github.com/Mr-xn/bc8261a5c3e35a72768723acf1da358d#wf_file_downloadaspx Exploit Third Party Advisory https://gist.github.com/Mr-xn/bc8261a5c3e35a72768723acf1da358d#wf_file_downloadaspx

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Releases Guidance on Credential Risks Associated with Potential Legacy Oracle Cloud Compromise	▪ Escalate privileges and move laterally within networks. ▪ Access cloud and identity management systems. ▪ Conduct phishing, credential-based, or business email compromise (BEC) campaigns. ▪ Resell or exchange access to stolen credentials on criminal marketplaces. ▪ Enrich stolen data with prior breach information for resale and/or targeted intrusion.	https://www.cisa.gov/news-events/alerts/2025/04/16/cisa-releases-guidance-credential-risks-associated-potential-legacy-oracle-cloud-compromise
CISA Adds One Known Exploited Vulnerability to Catalog	CVE-2021-20035	https://www.cisa.gov/news-events/alerts/2025/04/16/cisa-adds-one-known-exploited-vulnerability-catalog
CISA Releases Nine Industrial Control Systems Advisories	▪ ICSA-25-105-01 Siemens Mendix Runtime ▪ ICSA-25-105-02 Siemens Industrial Edge Device Kit ▪ ICSA-25-105-03 Siemens SIMOCODE, SIMATIC, SIPLUS, SIDOOR, SIWAREX ▪ ICSA-25-105-04 Growatt Cloud Applications ▪ ICSA-25-105-05 Lantronix Xport ▪ ICSA-25-105-06 National Instruments LabVIEW ▪ ICSA-25-105-07 Delta Electronics COMMGR ▪ ICSA-25-105-08 ABB M2M Gateway ▪ ICSA-25-105-09 Mitsubishi Electric Europe B.V. smartRTU	https://www.cisa.gov/news-events/alerts/2025/04/15/cisa-releases-nine-industrial-control-systems-advisories

News

Σύντομη περιγραφή / Τίτλος	URL
CISA's 11-Month extension ensures continuity of MITRE's CVE Program	https://securityaffairs.com/176608/security/cisas-11-month-extension-ensures-continuity-of-mitres-cve-program.html
Google Blocked 5.1B Harmful Ads and Suspended 39.2M Advertiser Accounts in 2024	https://thehackernews.com/2025/04/google-blocked-51b-harmful-ads-and.html
Jira Down – Atlassian Jira Outage Disrupts Dashboard Access for Users Globally	https://cybersecuritynews.com/jira-down/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
4chan Offline After Cyberattack: Hackers Claim Full Admin Access and Leak Internal Data	https://dailysecurityreview.com/security-spotlight/4chan-offline-after-cyberattack-hackers-claim-full-admin-access-and-leak-internal-data/
Endue Software Data Breach Exposes Health Information of Over 118,000 Patients Across U.S. Infusion Centers	https://dailysecurityreview.com/security-spotlight/endue-software-data-breach-exposes-health-information-of-over-118000-patients-across-u-s-infusion-centers/
Landmark Admin Data Breach: 1.6 Million Affected Individuals	https://dailysecurityreview.com/security-spotlight/landmark-admin-data-breach-1-6-million-affected-individuals/
MedEx Ambulance Data Breach: 118,000 Patient Records Exposed	https://dailysecurityreview.com/security-spotlight/medex-ambulance-data-breach-118000-patient-records-exposed/
Over 16,000 Fortinet devices compromised with symlink backdoor	https://www.bleepingcomputer.com/news/security/over-16-000-fortinet-devices-compromised-with-symlink-backdoor/
Hertz Data Breach Exposes Customer Information in Cleo Zero-Day Attack	https://www.infosecurity-magazine.com/news/hertz-data-breach-exposes-customer/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
CISA Flags Actively Exploited Vulnerability in SonicWall SMA Devices	https://thehackernews.com/2025/04/cisa-flags-actively-exploited.html
Cisco Webex Vulnerability Allows Code Execution via Weaponized Meeting Links	https://cybersecuritynews.com/cisco-webex-vulnerability/
Microsoft vulnerabilities: What's improved, what's at risk	https://www.helpnetsecurity.com/2025/04/17/beyondtrust-microsoft-vulnerabilities-report-2024/
New Windows Task Scheduler Bugs Let Attackers Bypass UAC and Tamper with Logs	https://thehackernews.com/2025/04/experts-uncover-four-new-privilege.html
New Windows Task Scheduler Bugs Let Attackers Bypass UAC and Tamper with Logs	https://thehackernews.com/2025/04/experts-uncover-four-new-privilege.html

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Apple Patches Two Actively Exploited iOS Flaws Used in Sophisticated Targeted Attacks	https://thehackernews.com/2025/04/apple-patches-two-actively-exploited.html
Apple fixes two zero-days exploited in targeted iPhone attacks	https://www.bleepingcomputer.com/news/security/apple-fixes-two-zero-days-exploited-in-targeted-iphone-attacks/
Microsoft: Some devices offered Windows 11 upgrades despite Intune blocks	https://www.bleepingcomputer.com/news/microsoft/microsoft-some-devices-offered-windows-11-upgrades-despite-intune-blocks/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Cyber Threats Against Energy Sector Surge as Global Tensions Mount	https://securityaffairs.com/176591/hacking/cyber-threats-against-energy-sector-surge-as-global-tensions-mount.html
China-Backed Hackers Exploit BRICKSTORM Backdoor to Spy on European Businesses	https://www.infosecurity-magazine.com/news/china-hackers-brickstorm-backdoor/
Interlock Ransomware Employs Multi-Stage Attack Via Legitimate Websites to Deliver Malicious Browser Updates	https://cybersecuritynews.com/interlock-ransomware-employs-multi-stage-attack/

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/