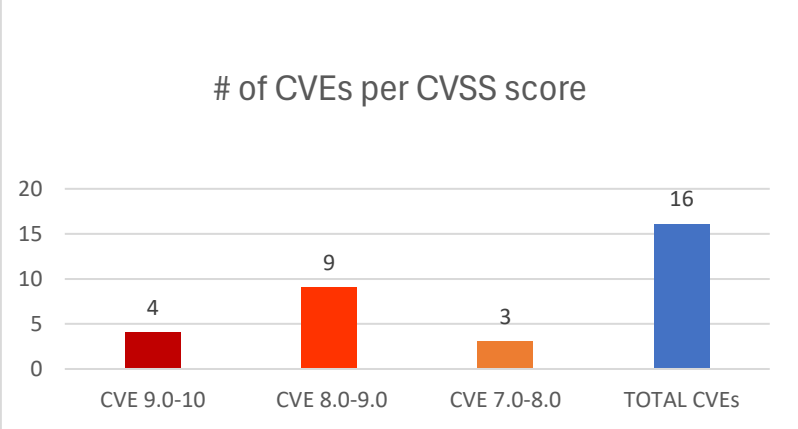
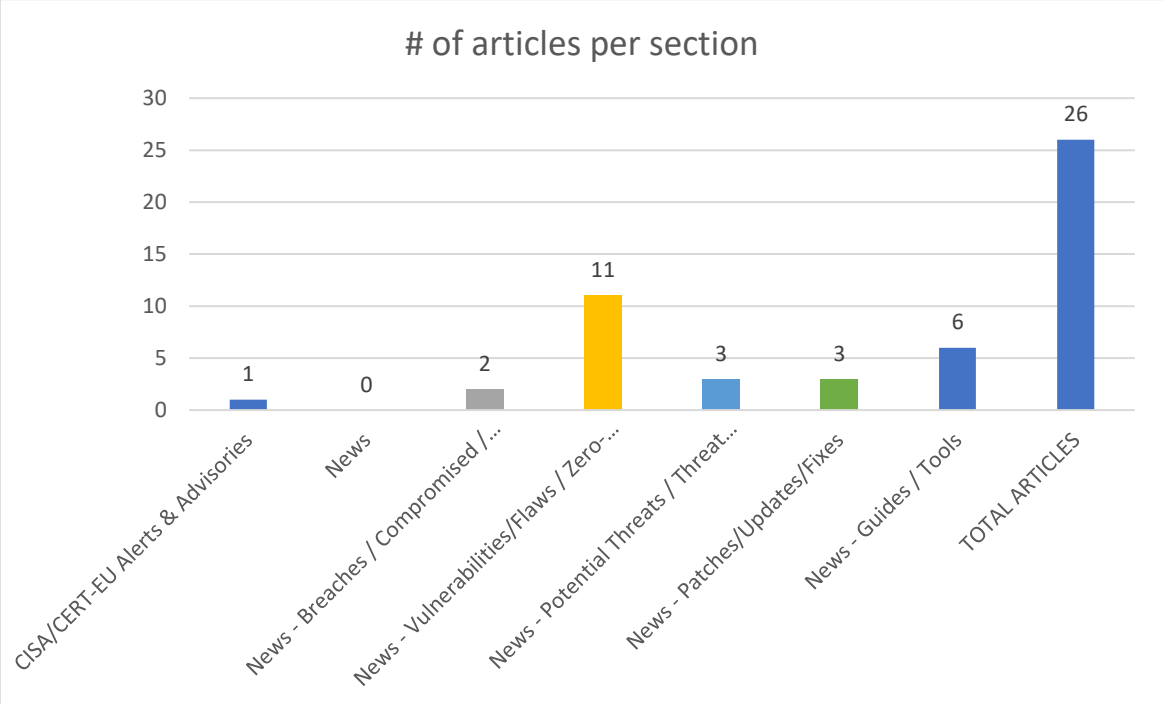
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 04/10/2025 - 07/10/2025





Contents

Common Vulnerabilities and Exposures (CVEs)

Η ενότητα αυτή εστιάζει σε ευπάθειες που έχουν καταχωρηθεί πρόσφατα και αξιολογούνται ως σοβαρές, με βάση τη βαθμολογία CVSS. Παρουσιάζονται με σαφήνεια τα συστήματα ή εφαρμογές που επηρεάζονται, ο τύπος της ευπάθειας (όπως SQL injection ή command injection) και σχετικοί σύνδεσμοι για περαιτέρω πληροφόρηση ή μέτρα αντιμετώπισης.

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-2025-9485	9,8	The OAuth Single Sign On – SSO (OAuth Client) plugin for WordPress	Improper Verification of Cryptographic Signature	versions up to, and including, 6.26.12	https://plugins.trac.wordpress.org/browser/miniorange-login-with-eve-online-google-facebook/tags/6.26.12/class-mooauth-widget.php#L577 Wordfence https://plugins.trac.wordpress.org/changeset/3360768/miniorange-login-with-eve-online-google-facebook Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/d2448afc-70d1-4dd5-b73b-62d182ee9a8a?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-61882	9,8	Oracle Concurrent Processing		12.2.3-12.2.14	https://www.oracle.com/security-alerts/alert-cve-2025-61882.html
https://nvd.nist.gov/vuln/detail/CVE-2025-57515	9,8	Uniclare Student Portal	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	v2	https://github.com/sanchitsahni/CVE-2025-57515/ MITRE https://github.com/sanchitsahni/CVE-2025-57515/blob/main/Uniclare%20Student%20Portal%20v2.pdf
https://nvd.nist.gov/vuln/detail/CVE-2025-61777	9,4	Flag Forge	Missing Authentication for Critical Function	version 2.0.0 and prior to version 2.3.2	https://github.com/FlagForgeCTF/flagForge/commit/e2121c5fb7a512a49dcd875812c944265fb1a846 GitHub, Inc. https://github.com/FlagForgeCTF/flagForge/security/advisories/GHSA-26rx-c53q-rjf9
https://nvd.nist.gov/vuln/detail/CVE-2025-11293	8,8	Belkin	Improper Restriction of Operations within the Bounds of a Memory Buffer	F9K1015 1.00.10	https://github.com/panda666-888/vuls/blob/main/belkin/f9k1015/formConnectionSetting.md VulDB https://github.com/panda666-888/vuls/blob/main/belkin/f9k1015/formConnectionSetting.md#poc VulDB https://vuldb.com/?ctiid.327174 VulDB https://vuldb.com/?id.327174 VulDB https://vuldb.com/?submit.661296

https://nvd.nist.gov/vuln/detail/CVE-2025-11325	8,8	Tenda AC18	Improper Restriction of Operations within the Bounds of a Memory Buffer	15.03.05.19(6318)	https://github.com/noahze01/IoT-vulnerable/blob/main/Tenda/AC18/fast_setting_pppoe_set.md VulDB https://vuldb.com/?ctiid.327208 VulDB https://vuldb.com/?id.327208 VulDB https://vuldb.com/?submit.664527 VulDB https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-11323	8,8	UTT 1250GW	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	up to v2v3.2.2-200710	https://github.com/DavCloudz/cve/issues/3 VulDB https://vuldb.com/?ctiid.327206 VulDB https://vuldb.com/?id.327206 VulDB https://vuldb.com/?submit.664524
https://nvd.nist.gov/vuln/detail/CVE-2025-11305	8,8	UTT HiPER 840G	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	up to 3.1.1-190328	https://github.com/maximdevere/CVE2/issues/3 VulDB https://vuldb.com/?ctiid.327186 VulDB https://vuldb.com/?id.327186 VulDB https://vuldb.com/?submit.661807
https://nvd.nist.gov/vuln/detail/CVE-2025-61673	8,6	Karapace	Missing Authentication for Critical Function	Versions 5.0.0 and 5.0.1	https://github.com/Aiven-Open/karapace/pull/1143/commits/c4038e9ce9fa504b433d59ac2944e337292922c7 GitHub, Inc. https://github.com/Aiven-Open/karapace/releases/tag/5.0.2 GitHub, Inc. https://github.com/Aiven-Open/karapace/security/advisories/GHSA-vq25-vcrw-gj53
https://nvd.nist.gov/vuln/detail/CVE-2025-29192	8,2	Flowise	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	before 3.0.5	https://github.com/FlowiseAI/Flowise/pull/4905 MITRE https://github.com/FlowiseAI/Flowise/releases/tag/flowise%403.0.5 MITRE https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-7r4h-vmj9-wg42
https://nvd.nist.gov/vuln/detail/CVE-2025-59943	8,1	phpMyFAQ	Incorrect User Management	Versions 4.0-nightly-2025-10-03 and below	https://github.com/thorsten/phpMyFAQ/commit/44cd20f86eb041f39d1c30a9beefad1cc61dc0ec GitHub, Inc. https://github.com/thorsten/phpMyFAQ/security/advisories/GHSA-9wj2-4hcm-r74j

https://nvd.nist.gov/vuln/detail/CVE-2025-9243	8,1	The Cost Calculator Builder plugin for WordPress	Missing Authorization	all versions up to, and including, 3.5.32	https://plugins.trac.wordpress.org/changeset/3371684/cost-calculator-builder#file388 Wordfence https://plugins.trac.wordpress.org/changeset/3371684/cost-calculator-builder#file389 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/aa46bdb3-6bbe-4f2f-8e1a-fbb54c5b39fd?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-59944	8,0	Cursor	Improper Handling of Case Sensitivity	Versions 1.6.23 and below	https://github.com/cursor/cursor/security/advisories/GHSA-xcwh-rrwj-gxc7
https://nvd.nist.gov/vuln/detail/CVE-2025-61679	7,7	Anyquery	Improper Authentication	Versions 0.4.3 and below	https://github.com/julien040/anyquery/commit/43cd8bd3354b9725b245a2354b08e1c9be1cc1d3 GitHub, Inc. https://github.com/julien040/anyquery/releases/tag/0.4.4 GitHub, Inc. https://github.com/julien040/anyquery/security/advisories/GHSA-5f7p-rhmq-hvc7
https://nvd.nist.gov/vuln/detail/CVE-2025-6985	7,5	The HTMLSectionSplitter	Improper Restriction of XML External Entity Reference	version 0.3.8	https://huntr.com/bounties/cf78abbb-df3b-43de-b6ee-132b73ff8331
https://nvd.nist.gov/vuln/detail/CVE-2025-60967	7,3	EndRun Technologies Sonoma D12 Network Time Server (GPS)	Cross Site Scripting (XSS)	F/W 6010-0076-000 Ver 4.00	http://endrun.com MITRE http://sonoma.com MITRE https://xdiv-sec.github.io/vulnerability-research/advisories/2025-10-03-sonoma-d12

CISA/CERT-EU Alerts & Advisories

Αυτό το κομμάτι περιλαμβάνει ειδοποιήσεις από επίσημες πηγές, κυρίως CISA και CERT-EU, σχετικά με κρίσιμες ευπάθειες ή ενεργές απειλές. Συνήθως αφορούν βιομηχανικά ή κρίσιμα συστήματα, αλλά και mainstream λογισμικό. Προσφέρονται σε μορφή σύντομων αναφορών και οδηγούν σε πιο λεπτομερείς τεχνικές οδηγίες.

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds Seven Known Exploited Vulnerabilities to Catalog	▪ **CVE-2010-3765 Mozilla Multiple Products Remote Code Execution Vulnerability** ▪ **CVE-2010-3962 Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability** ▪ **CVE-2011-3402 Microsoft Windows Remote Code Execution Vulnerability** ▪ **CVE-2013-3918 Microsoft Windows Out-of-Bounds Write Vulnerability** ▪ **CVE-2021-22555 Linux Kernel Heap Out-of-Bounds Write Vulnerability** ▪ **CVE-2021-43226 Microsoft Windows Privilege Escalation Vulnerability** ▪ **CVE-2025-61882 Oracle E-Business Suite Unspecified Vulnerability**	**https://www.cisa.gov/news-events/alerts/2025/10/06/cisa-adds-seven-known-exploited-vulnerabilities-catalog**

News

Η ενότητα "News" συνοψίζει τα πιο σημαντικά γεγονότα της εβδομάδας στον τομέα της κυβερνοασφάλειας. Εδώ θα βρείτε επιθέσεις που ξεχώρισαν, νέες τεχνικές που εντοπίστηκαν, ή ενέργειες από γνωστές ομάδες hacking. Δίνει την απαραίτητη εικόνα του τι συμβαίνει διεθνώς και πού πρέπει να στραφεί η προσοχή.

Σύντομη περιγραφή / Τίτλος	URL

Breaches / Compromised / Hacked

Καταγράφονται περιπτώσεις παραβίασης δεδομένων, διαρροών και άλλων σοβαρών περιστατικών ασφαλείας. Περιλαμβάνονται πληροφορίες για το ποιοι επηρεάστηκαν, με ποιον τρόπο έγινε η παραβίαση και πού υπάρχουν διαθέσιμες λεπτομέρειες. Είναι μια χρήσιμη εικόνα για να αντιληφθεί κανείς τη δυναμική των επιθέσεων σε πραγματικές συνθήκες.

Σύντομη περιγραφή / Τίτλος	URL
Renault Informs Customers of Supply Chain Data Breach	https://www.infosecurity-magazine.com/news/renault-customers-supply-chain/
Fort Wayne Medical Education Program notifies 29,000+ people of data breach	https://www.comparitech.com/news/fort-wayne-medical-education-program-notifies-29000-people-of-data-breach/?&web_view=true

Vulnerabilities / Flaws / Zero-day

Αναφέρονται τεχνικά ελαττώματα ή αδυναμίες που ενδέχεται να αξιοποιηθούν άμεσα από επιτιθέμενους — είτε επειδή είναι zero-day είτε γιατί η διόρθωσή τους καθυστερεί. Περιλαμβάνονται περιπτώσεις όπου δεν απαιτείται αλληλεπίδραση με τον χρήστη ή όπου παρακάμπτονται βασικά μέτρα ασφαλείας. Πολύ χρήσιμο για ομάδες που ασχολούνται με threat detection.

Σύντομη περιγραφή / Τίτλος	URL
Scanning Activity on Palo Alto Networks Portals Jump 500% in One Day	https://thehackernews.com/2025/10/scanning-activity-on-palo-alto-networks.html
Hackers exploited Zimbra flaw as zero-day using iCalendar files	https://www.bleepingcomputer.com/news/security/hackers-exploited-zimbra-flaw-as-zero-day-using-icalendar-files/
PoC Exploit Released for Sudo Vulnerability that Enables Attackers to Gain Root Access	https://cybersecuritynews.com/poc-exploit-sudo-vulnerability/
Redis Server Vulnerability use-after-free Vulnerability Enables Remote Code Execution	https://cybersecuritynews.com/redis-server-vulnerability/
QNAP NetBak Replicator Vulnerability Let Attackers Execute Unauthorized Code	https://cybersecuritynews.com/qnap-netbak-replicator-vulnerability/
PoC Exploit Released for Remotely Exploitable Oracle E-Business Suite 0-Day Vulnerability	https://cybersecuritynews.com/oracle-e-business-suite-0-day-vulnerability/
Unity Real-Time Development Platform Vulnerability Let Attackers Execute Arbitrary Code	https://cybersecuritynews.com/unity-real-time-development-platform-vulnerability/
Microsoft Links Storm-1175 to GoAnywhere Exploit Deploying Medusa Ransomware	https://thehackernews.com/2025/10/microsoft-links-storm-1175-to.html
Kibana Crowdstrike Connector Vulnerability Exposes Protected Credentials	https://cybersecuritynews.com/kibana-crowdstrike-connector-vulnerability/
CISA Warns of Windows Privilege Escalation Vulnerability Exploited in Attacks	https://cybersecuritynews.com/cisa-windows-privilege-escalation-vulnerability/
OpenSSH Vulnerability Exploited Via ProxyCommand to Execute Remote Code – PoC Released	https://cybersecuritynews.com/openssh-vulnerability-proxycommand/

Patches / Updates / Fixes

Εδώ θα βρείτε τις πιο πρόσφατες διορθώσεις και ενημερώσεις ασφαλείας από προμηθευτές λογισμικού και hardware. Το περιεχόμενο αφορά συγκεκριμένα bugs ή exploits που έχουν ήδη δημοσιοποιηθεί, μαζί με οδηγίες για το πώς να εφαρμοστούν τα patches.

Σύντομη περιγραφή / Τίτλος	URL
Oracle Rushes Patch for CVE-2025-61882 After Cl0p Exploited It in Data Theft Attacks	https://thehackernews.com/2025/10/oracle-rushes-patch-for-cve-2025-61882.html
Discord Data Breach – Customers Personal Data and Scanned Photo IDs leaked	https://cybersecuritynews.com/discord-data-breach/
Microsoft to Disable Inline SVG Images Display to Outlook for Web and Windows Users	https://cybersecuritynews.com/disable-svg-images-display-outlook/

Potential threats / Threat intelligence

Η συγκεκριμένη ενότητα ασχολείται με νέες απειλές, εξελιγμένα malware και τεχνικές επιθέσεων που έχουν εντοπιστεί σε πραγματικές συνθήκες. Περιλαμβάνονται αναφορές σε εργαλεία που χρησιμοποιούν οι επιτιθέμενοι, αλλά και δείκτες (IoCs) που μπορούν να χρησιμοποιηθούν στην άμυνα.

Σύντομη περιγραφή / Τίτλος	URL
Hackers Weaponize AWS X-Ray Service to Work as Covert Command & Control Server	https://cybersecuritynews.com/hackers-weaponize-aws-x-ray-service/
New WireTap Attack Break Server SGX To Exfiltrate Sensitive Data	https://cybersecuritynews.com/new-wiretap-attack/
New CometJacking Attack Let Attackers Turn Perplexity Browser Against You in One Click	https://cybersecuritynews.com/cometjacking-attack/

Guides / Tools

Παρουσιάζονται τεχνικοί οδηγοί και εργαλεία που μπορούν να βοηθήσουν στην παρακολούθηση, ανάλυση ή ενίσχυση της ασφάλειας συστημάτων. Είτε πρόκειται για open source projects είτε για νέες τεχνικές, η ενότητα αυτή λειτουργεί ως πόρος για πρακτικές λύσεις στην καθημερινή δουλειά των επαγγελματιών ασφάλειας.

Σύντομη περιγραφή / Τίτλος	URL
Top Tools for Enterprise Security Monitoring	**https://cybersecuritynews.com/enterprise-security-monitoring-tools/**
10 Best Vulnerability Management Tools In 2025	https://cybersecuritynews.com/vulnerability-management-tools/
Splunk Releases Guide to Detect Remote Employment Fraud Within Your Organization	https://cybersecuritynews.com/detect-remote-employment-fraud/
Top 15 Best Security Incident Response Tools In 2025	https://cybersecuritynews.com/incident-response-tools/
10 Best API Protection Tools in 2025	https://cybersecuritynews.com/best-api-protection-tools/
ThreatBook Launches Best-of-Breed Advanced Threat Intelligence Solution	https://cybersecuritynews.com/threatbook-advanced-threat-intelligence-solution/

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.

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/