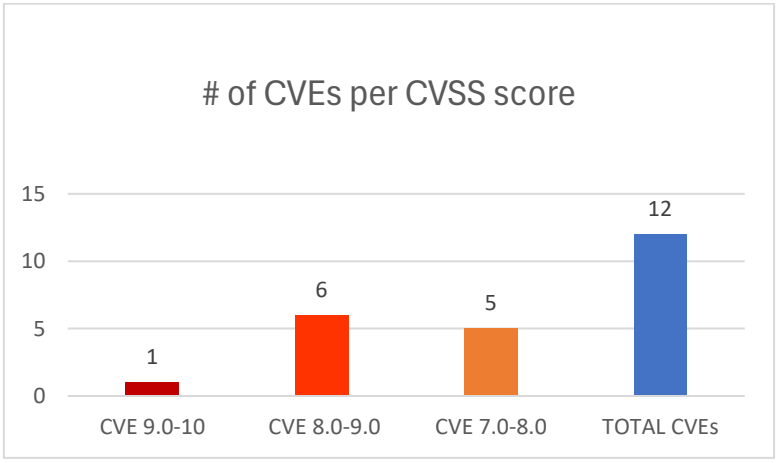
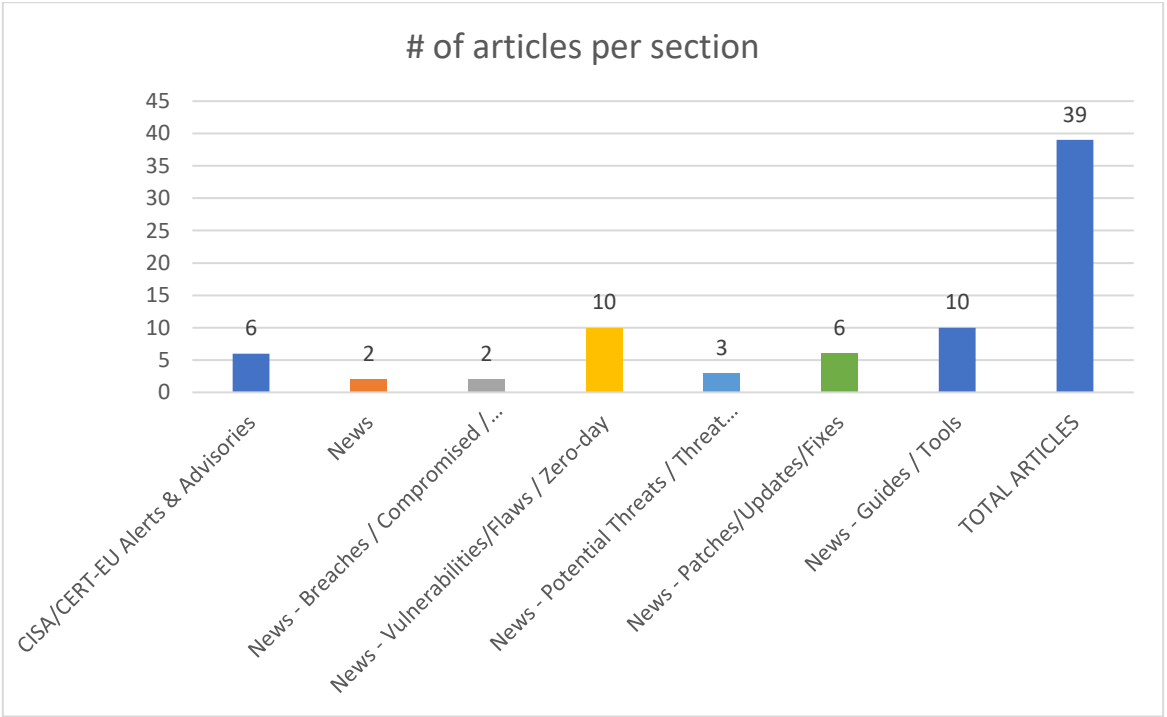
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 10/12/2025 - 12/12/2025





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-2025-67511	9,8	Cybersecurity AI (CAI)	Improper Neutralization of Special Elements used in a Command ('Command Injection')	0.5.9 and below	https://github.com/aliasrobotics/cai/commit/09ccb6e0baccf56c40e6cb429c698750843a999c GitHub, Inc. https://github.com/aliasrobotics/cai/security/advisories/GHSA-4c65-9gqf-4w8h
https://nvd.nist.gov/vuln/detail/CVE-2025-8405	8,7	GitLab	Improper Encoding or Escaping of Output	from 17.1 before 18.4.6, 18.5 before 18.5.4, and 18.6 before 18.6.2	https://about.gitlab.com/releases/2025/12/10/patch-release-gitlab-18-6-2-released/ GitLab Inc. https://gitlab.com/gitlab-org/gitlab/-/issues/558214 GitLab Inc. https://hackerone.com/reports/3270940
https://nvd.nist.gov/vuln/detail/CVE-2025-67738	8,5	squid/cachemgr.cgi in Webmin	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	before 2.600	https://github.com/webmin/webmin/commit/1a52bf4d72f9da6d79250c66e51f41c6f5b880ee MITRE https://github.com/webmin/webmin/compare/2.520...2.600
https://nvd.nist.gov/vuln/detail/CVE-2025-67505	8,4	Okta Java Management SDK	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11.0.0 through 20.0.0	https://github.com/okta/okta-sdk-java/commit/abf4f128a0441f90cb7efcdcf4bde1aef8703243 GitHub, Inc. https://github.com/okta/okta-sdk-java/security/advisories/GHSA-j5gq-897m-2rff
https://nvd.nist.gov/vuln/detail/CVE-2025-66675	8,2	Apache Struts	Incomplete Cleanup	from 2.0.0 through 6.7.4, from 7.0.0 through 7.0.3	https://cve.org/CVERecord?id=CVE-2025-64775 Apache Software Foundation https://cwiki.apache.org/confluence/display/WW/S2-068
https://nvd.nist.gov/vuln/d	8,2	Neuron	Improper Control of Generation of Code ('Code Injection')	2.8.11 and below	https://github.com/neuron-core/neuron-ai/commit/72735d0ea133266cf2f5d5d195d41e9dd865289a

etail/CVE-2025-67509					GitHub, Inc. https://github.com/neuron-core/neuron-ai/releases/tag/2.8.12 GitHub, Inc. https://github.com/neuron-core/neuron-ai/security/advisories/GHSA-j8g6-5gqc-mq36
https://nvd.nist.gov/vuln/detail/CVE-2025-67641	8,0	Jenkins Coverage Plugin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2.3054.ve1ff7b_a_a_123b_ and earlier	https://www.jenkins.io/security/advisory/2025-12-10/#SECURITY-3611
https://nvd.nist.gov/vuln/detail/CVE-2025-67460	7,8	Protection Mechanism Failure of Software Downgrade in Zoom Rooms for Windows	Protection Mechanism Failure	before 6.6.0	https://www.zoom.com/en/trust/security-bulletin/zsb-25050
https://nvd.nist.gov/vuln/detail/CVE-2025-65199	7,8	Windscribe for Linux Desktop App	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')		https://www.cve.org/CVERecord?id=CVE-2025-65199
https://nvd.nist.gov/vuln/detail/CVE-2025-66628	7,5	ImageMagick	Out-of-bounds Read	7.1.2-9 and prior	https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-6hjr-v6g4-3fm8 GitHub, Inc. https://github.com/dlemstra/Magick.NET/commit/2dfa08e15cfd11016a79615994787b14f9048b1c
https://nvd.nist.gov/vuln/detail/CVE-2025-67644	7,3	LangGraph SQLite	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	3.0.0	https://github.com/langchain-ai/langgraph/commit/297242913f8ad2143ee3e2f72e67db0911d48e2a GitHub, Inc. https://github.com/langchain-ai/langgraph/security/advisories/GHSA-9rwj-6rc7-p77c

https://nvd.nist.gov/vuln/detail/CVE-2025-67648	7,1	Shopware	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.4.6.0 through 6.6.10.9 and 6.7.0.0 through 6.7.5.0	https://github.com/shopware/shopware/commit/c9242c02c84595d9fa3e2adf6a264bc90a657b58 GitHub, Inc. https://github.com/shopware/shopware/security/advisories/GHSA-6w82-v552-wjw2

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 One Known Exploited Vulnerability to Catalog	▪ **CVE-2025-14174 Google Chromium Out-of-Bounds Memory Access Vulnerability**	**https://www.cisa.gov/news-events/alerts/2025/12/12/cisa-adds-one-known-exploited-vulnerability-catalog-0**
CISA Adds One Known Exploited Vulnerability to Catalog	▪ **CVE-2018-4063 Sierra Wireless AirLink ALEOS Unrestricted Upload of File with Dangerous Type Vulnerability**	**https://www.cisa.gov/news-events/alerts/2025/12/12/cisa-adds-one-known-exploited-vulnerability-catalog**
CISA Adds One Known Exploited Vulnerability to Catalog	▪ **CVE-2025-58360 OSGeo GeoServer Improper Restriction of XML External Entity Reference Vulnerability**	**https://www.cisa.gov/news-events/alerts/2025/12/11/cisa-adds-one-known-exploited-vulnerability-catalog**
CISA Releases 12 Industrial Control Systems Advisories	▪ **ICSA-25-345-01 Johnson Controls iSTAR** ▪ **ICSA-25-345-02 Johnson Controls iSTAR Ultra** ▪ **ICSA-25-345-03 AzeoTech DAQFactory** ▪ **ICSA-25-345-04 Siemens IAM Client** ▪ **ICSA-25-345-05 Siemens Advanced Licensing (SALT) Toolkit** ▪ **ICSA-25-345-06 Siemens SINEMA Remote Connect Server**	**https://www.cisa.gov/news-events/alerts/2025/12/11/cisa-releases-12-industrial-control-systems-advisories**

	▪ ICSA-25-345-07 Siemens Building X - Security Manager Edge Controller ▪ ICSA-25-345-08 Siemens Energy Services ▪ ICSA-25-345-09 Siemens Gridscale X Prepay ▪ ICSA-25-345-10 OpenPLC_V3 ▪ ICSMA-25-345-01 Grassroots DICOM (GDCM) ▪ ICSMA-25-345-02 Varex Imaging Panoramic Dental Imaging Software	
2025 CWE Top 25 Most Dangerous Software Weaknesses	▪	https://www.cisa.gov/news-events/alerts/2025/12/11/2025-cwe-top-25-most-dangerous-software-weaknesses
Cybersecurity Performance Goals 2.0 for Critical Infrastructure	▪	https://www.cisa.gov/news-events/alerts/2025/12/11/cybersecurity-performance-goals-20-critical-infrastructure

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
Pro-Russia Hackers Target US Critical Infrastructure in New Wave	https://www.infosecurity-magazine.com/news/russia-hackers-target-us-critical/
What's Next for SOC in 2026: Get the Early-Adopter Advantage	https://cybersecuritynews.com/whats-next-for-soc-in-2026-get-the-early-adopter-advantage/

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
Ransomware gang says it hacked Kansas broadband provider Rainbow Communications	https://www.comparitech.com/news/ransomware-gang-says-it-hacked-kansas-broadband-provider-rainbow-communications/?&web_view=true
Petco takes down Vetco website after exposing customers' personal information	https://techcrunch.com/2025/12/10/petco-takes-down-vetco-website-after-exposing-customers-personal-information/?&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
Chrome Targeted by Active In-the-Wild Exploit Tied to Undisclosed High-Severity Flaw	https://thehackernews.com/2025/12/chrome-targeted-by-active-in-wild.html
Fortinet, Ivanti, and SAP Issue Urgent Patches for Authentication and Code Execution Flaws	https://thehackernews.com/2025/12/fortinet-ivanti-and-sap-issue-urgent.html
Warning: WinRAR Vulnerability CVE-2025-6218 Under Active Attack by Multiple Threat Groups	https://thehackernews.com/2025/12/warning-winrar-vulnerability-cve-2025.html
Three PCIe Encryption Weaknesses Expose PCIe 5.0+ Systems to Faulty Data Handling	https://thehackernews.com/2025/12/three-pcie-encryption-weaknesses-expose.html
React2Shell Exploitation Delivers Crypto Miners and New Malware Across Multiple Sectors	https://thehackernews.com/2025/12/react2shell-exploitation-delivers.html
Over 644,000 Domains Exposed to Critical React Server Components Vulnerability	https://cybersecuritynews.com/react-server-vulnerability-domains-exposed/
Windows Defender Firewall Service Vulnerability Let Attackers Disclose Sensitive Data	https://cybersecuritynews.com/windows-defender-firewall-service-vulnerability/
Adobe Acrobat Reader Vulnerabilities Let Attackers Execute Arbitrary Code and Bypass Security	https://cybersecuritynews.com/adobe-acrobat-reader-vulnerabilities-code/
Microsoft Outlook Vulnerability Let Attackers Execute Malicious Code Remotely	https://cybersecuritynews.com/microsoft-outlook-vulnerability/
Windows PowerShell 0-Day Vulnerability Let Attackers Execute Malicious Code	https://cybersecuritynews.com/windows-powershell-0-day-vulnerability/

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
Microsoft Issues Security Fixes for 56 Flaws, Including Active Exploit and Two Zero-Days	https://thehackernews.com/2025/12/microsoft-issues-security-fixes-for-56.html
Google Patches Mysterious Chrome Zero-Day Exploited in the Wild	https://www.securityweek.com/google-patches-mysterious-chrome-zero-day-exploited-in-the-wild/
SAP Patches Critical Vulnerabilities With December 2025 Security Updates	https://www.securityweek.com/sap-patches-critical-vulnerabilities-with-december-2025-security-updates/
Ivanti EPM Update Patches Critical Remote Code Execution Flaw	https://www.securityweek.com/ivanti-epm-update-patches-critical-remote-code-execution-flaw/
Fortinet Patches Critical Authentication Bypass Vulnerabilities	https://www.securityweek.com/fortinet-patches-critical-authentication-bypass-vulnerabilities/
Google Fixes Zero Click Gemini Enterprise Flaw That Exposed Corporate Data	https://www.infosecurity-magazine.com/news/google-fixes-gemini-enterprise-flaw/

Potential threats / Threat intelligence

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

Σύντομη περιγραφή / Τίτλος	URL
ClickFix Style Attack Uses Grok, ChatGPT for Malware Delivery	https://www.darkreading.com/vulnerabilities-threats/clickfix-style-attack-grok-chatgpt-malware
ClickFix Social Engineering Sparks Rise of CastleLoader Attacks	**https://www.infosecurity-magazine.com/news/clickfix-rise-castleloader-attacks/**
Hackers Infiltrate VS Code Marketplace with 19 Malicious Extensions Posing as PNG File	https://cybersecuritynews.com/hackers-infiltrate-vs-code-marketplace/

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/
CISA Releases Best Security Practices Guide for Hardening Microsoft Exchange Server	https://cybersecuritynews.com/microsoft-exchange-server-hardening-guide/
15 Best Remote Monitoring Tools – 2025	https://cybersecuritynews.com/best-remote-monitoring-tools/
Top 10 Best Exposure Management Tools In 2026	https://cybersecuritynews.com/best-exposure-management-tools/
NETREAPER Offensive Security Toolkit That Wraps 70+ Penetration Testing Tools	https://cybersecuritynews.com/netreaper-offensive-security-toolkit/

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/