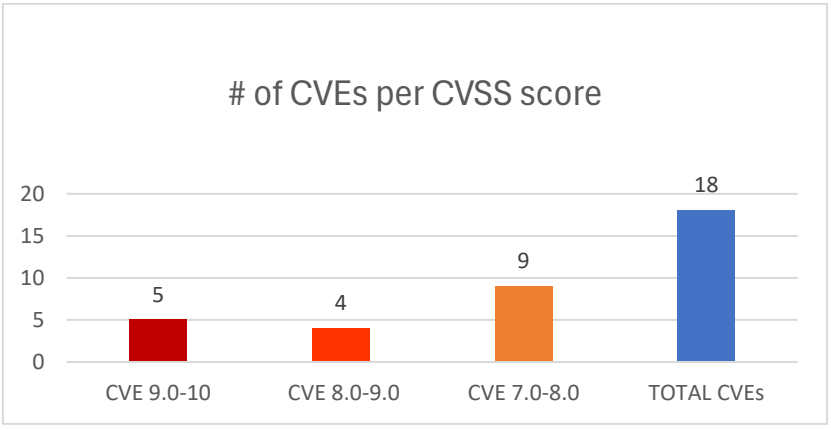
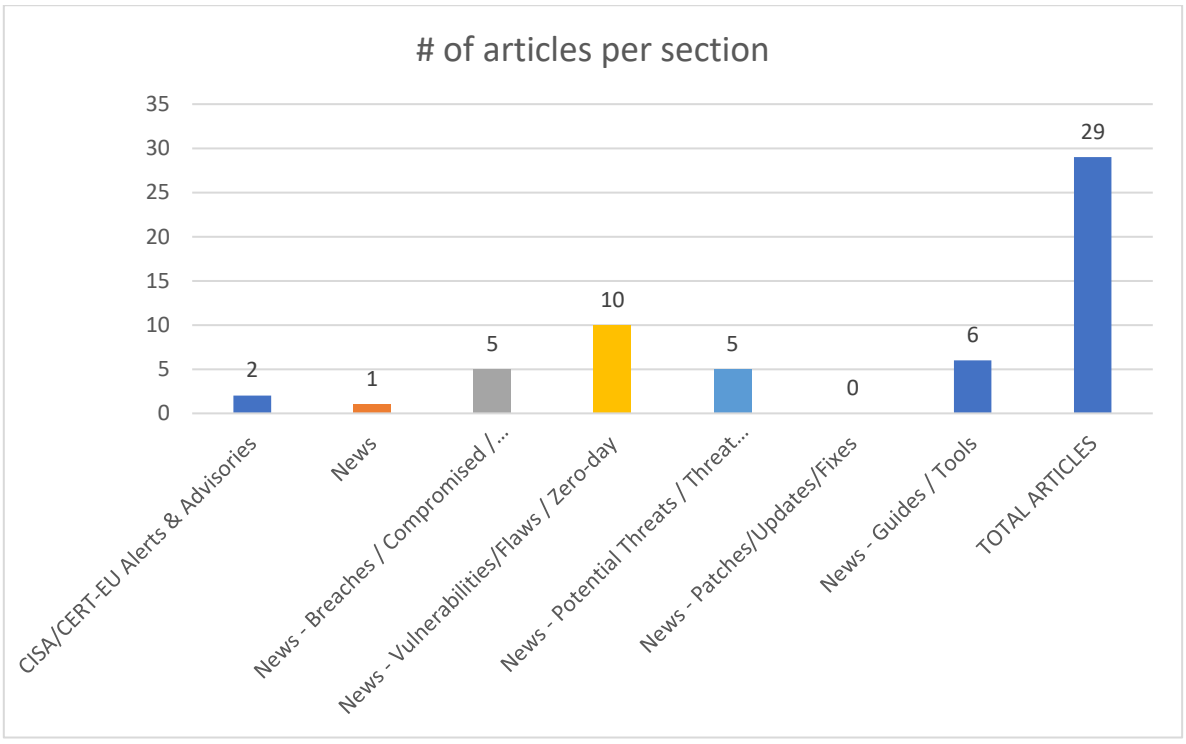
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 27/12/2025 - 31/12/2025





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-2025-54322	10,0	Xspeeder SXZOS	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	through 2025-12-26	https://pwn.ai/blog/cve-2025-54322-zeroday-unauthenticated-root-rce-affecting-70-000-hosts CISA-ADP, MITRE https://www.xspeeder.com
https://nvd.nist.gov/vuln/detail/CVE-2025-66203	9,9	StreamVault	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Prior to version 251126	https://github.com/lemon8866/StreamVault/releases/tag/251226 GitHub, Inc. https://github.com/lemon8866/StreamVault/security/advisories/GHSA-c747-q388-3v6m
https://nvd.nist.gov/vuln/detail/CVE-2024-44065	9,8	Cloudlog	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	v2.6.15	https://github.com/jacopo1223/jacopo.github/tree/main/CVE-2024-44065 MITRE https://github.com/magicbug/Cloudlog
https://nvd.nist.gov/vuln/detail/CVE-2025-68990	9,8	xenioushk BWL Pro Voting Manager bwl-pro-voting-manager	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	from n/a through <= 1.4.9	https://vdp.patchstack.com/database/Wordpress/Plugin/bwl-pro-voting-manager/vulnerability/wordpress-bwl-pro-voting-manager-plugin-1-4-9-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-68974	9,8	WordPress Social Login and Register	Improper Control of Filename for Include/Require Statement in PHP	from n/a through <= 7.7.0	https://vdp.patchstack.com/database/Wordpress/Plugin/miniorange-login-openid/vulnerability/wordpress-wordpress-social-login-and-register-plugin-7-7-0-local-file-inclusion-vulnerability?_s_id=cve

			Program ('PHP Remote File Inclusion		
https://nvd.nist.gov/vuln/detail/CVE-2025-67729	8,8	LMDeploy	Deserialization of Untrusted Data	Prior to version 0.11.1	https://github.com/InternLM/lmdeploy/commit/eb04b4281c5784a5cff5ea639c8f96b33b3ae5ee GitHub, Inc. https://github.com/InternLM/lmdeploy/security/advisories/GHSA-9pf3-7rrr-x5jh
https://nvd.nist.gov/vuln/detail/CVE-2025-68975	8,1	Eagle Booking	Authorization Bypass Through User-Controlled Key	from n/a through <= 1.3.4.3	https://vdp.patchstack.com/database/Wordpress/Plugin/eagle-booking/vulnerability/wordpress-eagle-booking-plugin-1-3-4-3-insecure-direct-object-references-idor-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-68979	8,1	Google Calendar Events	Authorization Bypass Through User-Controlled Key	from n/a through <= 3.5.9	https://vdp.patchstack.com/database/Wordpress/Plugin/google-calendar-events/vulnerability/wordpress-google-calendar-events-plugin-3-5-9-insecure-direct-object-references-idor-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-68980	8,1	WeDesignTech Portfolio	Missing Authorization	from n/a through <= 1.0.2	https://vdp.patchstack.com/database/Wordpress/Plugin/wedesigntech-portfolio/vulnerability/wordpress-wedesigntech-portfolio-plugin-1-0-2-broken-access-control-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-68973	7,8	GnuPG	Multiple Operations on Resource in Single-Operation Context	before 2.4.9	http://www.openwall.com/lists/oss-security/2025/12/29/11 CVE https://github.com/gpg/gnupg/blob/ff306834186955f5d2cc9e6cf8c9418e09378ebe4/g10/armor.c#L1305-L1306 MITRE https://github.com/gpg/gnupg/commit/115d138ba599328005c5321c0ef9f00355838ca9 MITRE https://github.com/gpg/gnupg/compare/gnupg-2.2.50...gnupg-2.2.51 MITRE https://gpg.fail/memcpy CISA-ADP, MITRE https://news.ycombinator.com/item?id=46403200

					MITRE https://www.openwall.com/lists/oss-security/2025/12/28/5
https://nvd.nist.gov/vuln/detail/CVE-2025-69256	7,5	The Serverless Framework	Improper Neutralization of Special Elements used in a Command ('Command Injection')	4.29.0 and prior to version 4.29.3	https://github.com/serverless/serverless/blob/6213453da7df375aaf12fb3522ab8870488fc59a/packages/mcp/src/tools/list-projects.js#L68 GitHub, Inc. https://github.com/serverless/serverless/commit/681ca039550c7169369f98780c6301a00f2dc4c4 GitHub, Inc. https://github.com/serverless/serverless/releases/tag/sf-core%404.29.3 GitHub, Inc. https://github.com/serverless/serverless/security/advisories/GHSA-rwc2-f344-q6w6
https://nvd.nist.gov/vuln/detail/CVE-2025-69200	7,5	phpMyFAQ	Exposure of Sensitive Information Through Data Queries	prior to 4.0.16	https://github.com/thorsten/phpMyFAQ/commit/b0e99ee3695152115841cb546d8dce64ceb8c29a GitHub, Inc. https://github.com/thorsten/phpMyFAQ/security/advisories/GHSA-9cg9-4h4f-j6fg
https://nvd.nist.gov/vuln/detail/CVE-2025-59946	7,5	NanoMQ MQTT Broker (NanoMQ)	Use After Free	Prior to version 0.24.2	https://github.com/nanomq/nanomq/issues/1863 GitHub, Inc. https://github.com/nanomq/nanomq/security/advisories/GHSA-xg37-23w7-72p5
https://nvd.nist.gov/vuln/detail/CVE-2025-67015	7,5	Comtech EF Data CDM-625 / CDM-625A Advanced Satellite Modem	Improper Access Control	v2.5.1	https://github.com/shiky8/my--cve-vulnerability-research/tree/main/CVE-2025-67015%20_%20Comtech%20EF%20Data%20CDM-625%20_%20CDM-625A%20Advanced%20_%20Broken%20Access%20Control MITRE https://www.comtechefdata.com/

https://nvd.nist.gov/vuln/detail/CVE-2025-67014	7,5	DEV Systemtechnik GmbH DEV 7113 RF	Improper Access Control		https://dev-systemtechnik.com MITRE https://github.com/shiky8/my--cve-vulnerability-research/tree/main/CVE-2025-67014%20_%20DEV%20Systemtechnik%20GmbH%20DEV%207113%20RF%20over%20_%20Broken%20Access%20Control MITRE
https://nvd.nist.gov/vuln/detail/CVE-2025-68989	7,5	Renzo Johnson Contact Form 7 Extension For Mailchimp contact-form-7-mailchimp-extension	Insertion of Sensitive Information Into Sent Data	from n/a through <= 0.9.49.	https://vdp.patchstack.com/database/Wordpress/Plugin/contact-form-7-mailchimp-extension/vulnerability/wordpress-contact-form-7-extension-for-mailchimp-plugin-0-9-49-sensitive-data-exposure-vulnerability?_s_id=cve]
https://nvd.nist.gov/vuln/detail/CVE-2025-68988	7,5	E-Invoice App Malaysia	Exposure of Sensitive System Information to an Unauthorized Control Sphere	from n/a through <= 1.1.0	https://vdp.patchstack.com/database/Wordpress/Plugin/einvoiceapp-malaysia/vulnerability/wordpress-e-invoice-app-malaysia-plugin-1-1-0-sensitive-data-exposure-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-61914	7,3	n8n	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Prior to version 1.114.0	https://github.com/n8n-io/n8n/security/advisories/GHSA-58jc-rcg5-95f3

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 Releases Two Industrial Control Systems Advisories	▪ **ICSA-25-364-01: WHILL C2 Wheelchairs** ▪ **ICSA-25-345-03: AzeoTech DAQFactory (Update A)**	**https://www.cisa.gov/news-events/alerts/2025/12/30/cisa-releases-two-industrial-control-systems-advisories**
CISA Adds One Known Exploited Vulnerability to Catalog	▪ **CVE-2025-14847 MongoDB and MongoDB Server Improper Handling of Length Parameter Inconsistency Vulnerability**	**https://www.cisa.gov/news-events/alerts/2025/12/29/cisa-adds-one-known-exploited-vulnerability-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
OpenAI Hardened ChatGPT Atlas Against Prompt Injection Attacks	**https://cybersecuritynews.com/openai-hardened-chatgpt-atlas/**

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
Korean Air discloses data breach after the hack of its catering and duty-free supplier	**https://securityaffairs.com/186275/data-breach/korean-air-discloses-data-breach-after-the-hack-of-its-catering-and-duty-free-supplier.html?&web_view=true**
Two more banks notifying thousands of victims about Marquis Software ransomware attack	**https://therecord.media/banks-marquis-software-ransomware?&web_view=true**

European Space Agency Confirms Breach of Servers Outside the Corporate Network	**https://cybersecuritynews.com/european-space-agency-breach/**
Hackers Claim Breach of WIRED Database Containing 2.3 million Subscriber Records	https://cybersecuritynews.com/wired-database-breach/
Hackers Infiltrated Maven Central Masquerading as a Legitimate Jackson JSON Library	https://cybersecuritynews.com/hackers-infiltrated-maven-central/

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
Fortinet Warns of New Attacks Exploiting Old Vulnerability	**https://www.securityweek.com/fortinet-warns-of-new-attacks-exploiting-old-vulnerability/**
Fresh MongoDB Vulnerability Exploited in Attacks	**https://www.securityweek.com/fresh-mongodb-vulnerability-exploited-in-attacks/**
Critical Vulnerability in SmarterMail Let Attackers Execute Remote Code	**https://cybersecuritynews.com/smartermail-vulnerability/**
CISA Warns of MongoDB Server Vulnerability(CVE-2025-14847) Exploited in Attacks	**https://cybersecuritynews.com/cisa-mongodb-server-vulnerability/**
70,000+ MongoDB Servers Vulnerable to MongoBleed Exploit – PoC Released	**https://cybersecuritynews.com/70000-mongodb-servers-vulnerable/**
TeamViewer DEX Vulnerabilities Let Attackers Trigger DoS Attack and Expose Sensitive Data	**https://cybersecuritynews.com/teamviewer-dex-vulnerabilities/**
M-Files Vulnerability Let Attacker Capture Session Tokens of Other Active Users	**https://cybersecuritynews.com/m-files-vulnerability/**
Windows Vulnerabilities via Kernel Drivers and Named Pipes Allows Privilege Escalation	**https://cybersecuritynews.com/windows-lpe-vulnerabilities/**
New Vulnerabilities in Bluetooth Headphones Let Hackers Hijack Connected Smartphone	**https://cybersecuritynews.com/bluetooth-headphones-vulnerabilities/**
2.5 Million+ Malicious Request From Hackers Attacking Adobe ColdFusion Servers	**https://cybersecuritynews.com/coldfusion-servers-under-attack/**

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

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 Advertised VOID 'AV Killer' with Kernel-level Termination Claims	https://cybersecuritynews.com/hackers-advertised-void-av-killer/
Massive Magecart with 50+ Malicious Scripts Hijacking Checkout and Account Creation Flows	https://cybersecuritynews.com/massive-magecart-with-50-malicious-scripts/
ESET Warns AI-driven Malware Attack and Rapidly Growing Ransomware Economy	https://cybersecuritynews.com/eset-warns-ai-driven-malware-attack/
Hackers Exploit Copilot Studio's New Connected Agents Feature to Gain Backdoor Access	https://cybersecuritynews.com/hackers-exploit-copilot-studios-new-connected-agents-feature/
Silver Fox Hackers Attacking Indian Entities with Income Tax Phishing Lures	https://cybersecuritynews.com/silver-fox-hackers-attacking-indian-entities/

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/