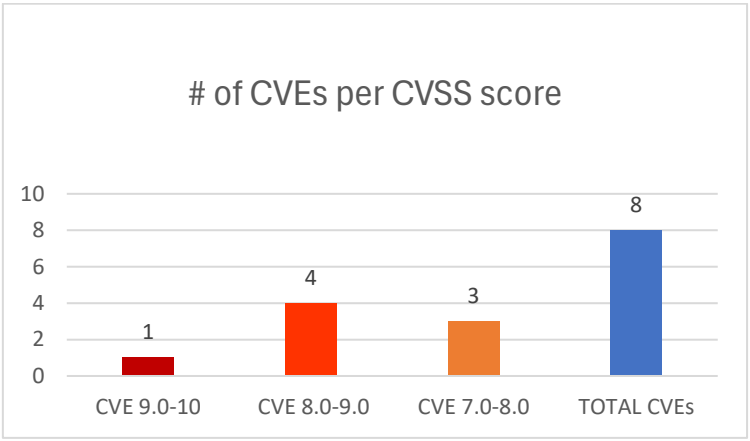
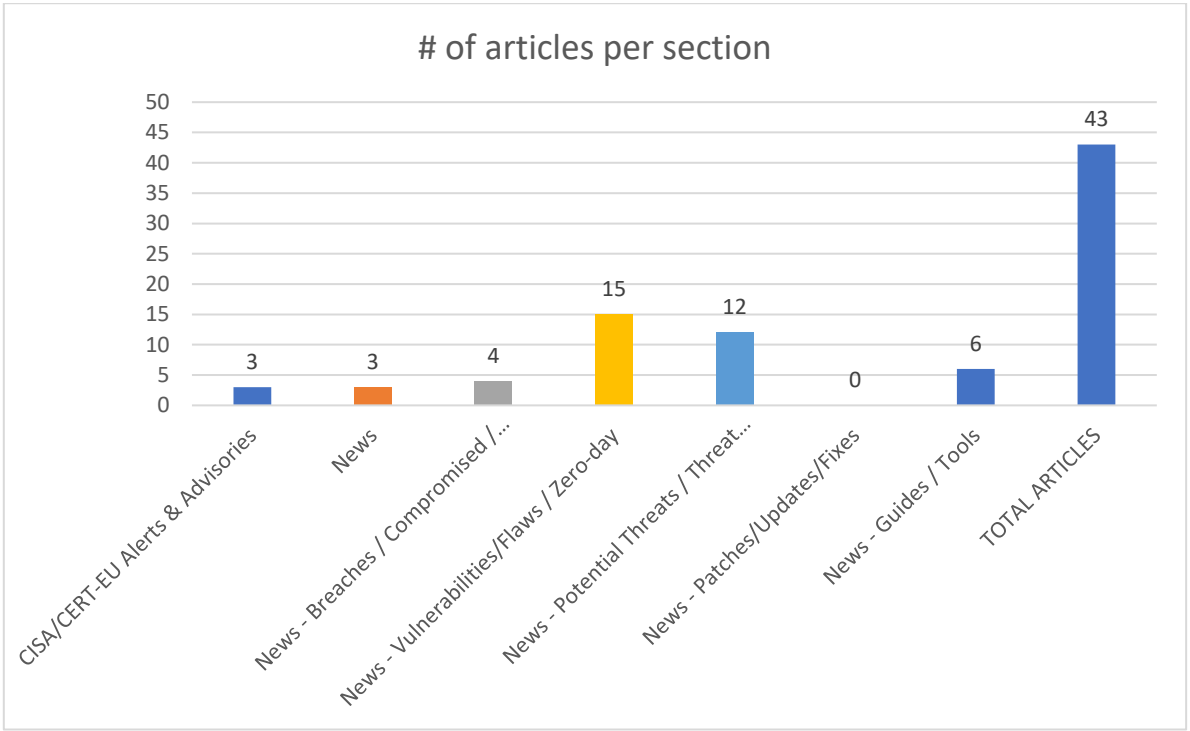
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 27/09/2025 - 30/09/2025





Contents

Common Vulnerabilities and Exposures (CVEs) 3
CISA/CERT-EU Alerts & Advisories 5
News 5
Breaches / Compromised / Hacked 6
Vulnerabilities / Flaws / Zero-day 6
Patches / Updates / Fixes 7
Potential threats / Threat intelligence 7
Guides / Tools 8
References 9
Annex – Websites with vendor specific vulnerabilities 10

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-2025-59934	9,4	Formbricks	Improper Authentication	Prior to version 4.0.1	https://github.com/formbricks/formbricks/blob/843110b0d6c37b5c0da54291616f84c91c55c4fc/apps/web/lib/jwt.ts#L114-L117 GitHub, Inc. https://github.com/formbricks/formbricks/commit/eb1349f205189d5b2d4a95ec42245ca98cf68c82 GitHub, Inc. https://github.com/formbricks/formbricks/pull/6596 GitHub, Inc. https://github.com/formbricks/formbricks/security/advisories/GHSA-7229-q9pv-j6p4
https://nvd.nist.gov/vuln/detail/CVE-2025-59939	8,8	WeGIA	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Prior to version 3.5.0	https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-jx9m-pgf8-v489
https://nvd.nist.gov/vuln/detail/CVE-2025-11091	8,8	Tenda AC21	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	up to 16.03.08.16	https://github.com/maximdevere/CVE2/issues/2 VulDB https://vuldb.com/?ctiid.326173 VulDB https://vuldb.com/?id.326173 VulDB https://vuldb.com/?submit.661806 VulDB https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-59932	8,6	Flag Forge is a Capture The Flag (CTF) platform	Improper Access Control	From versions 2.0.0 to before 2.3.1	https://github.com/FlagForgeCTF/flagForge/security/advisories/GHSA-v8rh-25rf-gfqw
https://nvd.nist.gov/vuln/detail/CVE-2025-59945	8,1	SysReptor	Incorrect Privilege Assignment	In versions from 2024.74 to before 2025.83	https://github.com/Syslifters/sysreptor/commit/de8b5d89d0644479ee0da0a113c6bcc2436ba7f4 GitHub, Inc. https://github.com/Syslifters/sysreptor/security/advisories/GHSA-r6hm-59cq-gjg6

https://nvd.nist.gov/vuln/detail/CVE-2025-8014	7,5	Denial of Service issue in GraphQL endpoints in Gitlab EE/CE	Allocation of Resources Without Limits or Throttling	all versions from 11.10 prior to 18.2.7, 18.3 prior to 18.3.3, and 18.4 prior to 18.4.1	https://gitlab.com/gitlab-org/gitlab/-/issues/556838 GitLab Inc. https://hackerone.com/reports/3228134
https://nvd.nist.gov/vuln/detail/CVE-2025-7647	7,3	The llama-index-core package	Creation of Temporary File With Insecure Permissions	up to version 0.12.44	https://github.com/run-llama/llama_index/commit/98816394d57c7f53f847ed7b60725e69d0e7aae4 huntr.dev https://huntr.com/bounties/a2baa08f-98bf-47a8-ac83-06f7411afd9e
https://nvd.nist.gov/vuln/detail/CVE-2025-9816	7,2	The WP Statistics – The Most Popular Privacy-Friendly Analytics Plugin plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	all versions up to, and including, 14.5.4	https://plugins.trac.wordpress.org/browser/wp-statistics/tags/14.15.3/includes/admin/templates/pages/devices/models.php#L31 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/d8351204-da6d-443a-98b5-0608bfb1e9d0?source=cve

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 and UK NCSC Release Joint Guidance for Securing OT Systems		**https://www.cisa.gov/news-events/alerts/2025/09/29/cisa-and-uk-ncsc-release-joint-guidance-securing-ot-systems**
CISA Strengthens Commitment to SLTT Governments		**https://www.cisa.gov/news-events/alerts/2025/09/29/cisa-strengthens-commitment-sltt-governments**
CISA Adds Five Known Exploited Vulnerabilities to Catalog	▪ **CVE-2021-21311 Adminer Server-Side Request Forgery Vulnerability** ▪ **CVE-2025-20352 Cisco IOS and IOS XE Stack-based Buffer Overflow Vulnerability** ▪ **CVE-2025-10035 Fortra GoAnywhere MFT Deserialization of Untrusted Data Vulnerability** ▪ **CVE-2025-59689 Libraesva Email Security Gateway Command Injection Vulnerability** ▪ **CVE-2025-32463 Sudo Inclusion of Functionality from Untrusted Control Sphere Vulnerability**	**https://www.cisa.gov/news-events/alerts/2025/09/29/cisa-adds-five-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
Can We Trust AI To Write Vulnerability Checks? Here's What We Found	**https://www.bleepingcomputer.com/news/security/can-we-trust-ai-to-write-vulnerability-checks-heres-what-we-found/**
AI-Generated Code Used in Phishing Campaign Blocked by Microsoft	https://www.infosecurity-magazine.com/news/ai-generated-code-phishing/
Two-Thirds of Organizations Have Unfilled Cybersecurity Positions	https://www.infosecurity-magazine.com/news/two-thirds-unfilled-cybersecurity/

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
Chinese Cyberspies Hacked US Defense Contractors	https://www.securityweek.com/chinese-cyberspies-hacked-us-defense-contractors/?&web_view=true
Harrods Reveals Supply Chain Breach Impacting Online Customers	https://www.infosecurity-magazine.com/news/harrods-supply-chain-breach-online/
DataCenter Fire Takes 600+ South Korean Government Websites Offline	https://cybersecuritynews.com/datacenter-fire/
Medusa Ransomware Claims Comcast Data Breach, Demands $1.2M	https://hackread.com/medusa-ransomware-comcast-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
Apache Airflow Vulnerability Exposes Sensitive Details to Read-Only Users	https://cybersecuritynews.com/apache-airflow-vulnerability/
Google Project Zero Details ASLR Bypass on Apple Devices Using NSDictionary Serialization	https://cybersecuritynews.com/aslr-bypass-on-apple-devices/
Cybersecurity Newsletter Weekly – Chrome 0-Day, 22.2 Tbps DDOS Attack, Kali Linux Release, Cisco IOS 0-Day and More	https://cybersecuritynews.com/cybersecurity-newsletter-september/
CISA Sounds Alarm on Critical Sudo Flaw Actively Exploited in Linux and Unix Systems	https://thehackernews.com/2025/09/cisa-sounds-alarm-on-critical-sudo-flaw.html
First Malicious MCP Server Found Stealing Emails in Rogue Postmark-MCP Package	https://thehackernews.com/2025/09/first-malicious-mcp-server-found.html
VMware vCenter and NSX Vulnerabilities Let Attackers Enumerate Valid Usernames	https://cybersecuritynews.com/vmware-vcenter-and-nsx-vulnerabilities/
WhatsApp 0-Click Vulnerability Exploited Using Malicious DNG File	https://cybersecuritynews.com/whatsapp-0-click-vulnerability-exploited/
SUSE Rancher Vulnerabilities Let Attackers Lockout the Administrators Account	https://cybersecuritynews.com/suse-rancher-vulnerabilities/
Lesson From Cisco ASA 0-Day RCE Vulnerability That Actively Exploited In The Wild	https://cybersecuritynews.com/lessons-cisco-asa-0-day-rce-vulnerability/

Windows Heap Exploitation Vulnerability With Record's Size Field Leads to Arbitrary R/W	https://cybersecuritynews.com/windows-heap-exploitation-vulnerability/
Formbricks Signature Verification Vulnerability Let Attackers Reset User Passwords Without Authorization	https://cybersecuritynews.com/formbricks-signature-verification-vulnerability/
Notepad++ DLL Hijacking Vulnerability Let Attackers Execute Malicious Code	https://cybersecuritynews.com/notepad-hijacking-vulnerability/
Apple Font Parser Vulnerability Enables Malicious Fonts to Corrupt Process Memory	https://cybersecuritynews.com/apple-font-parser-vulnerability/
Critical Western Digital My Cloud NAS Vulnerability Allows Remote Code Execution	https://cybersecuritynews.com/western-digital-my-cloud-devices-vulnerability/
VMware Tools and Aria Operations Vulnerabilities Let Attackers Escalate Privileges to Root	https://cybersecuritynews.com/vmware-tools-and-aria-operations-vulnerabilities/

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
LummaStealer Technical Details Uncovered Using ML-Based Detection Approach	https://cybersecuritynews.com/lummastealer-technical-details-uncovered/
Threat Actors Exploiting SonicWall Firewalls to Deploy Akira Ransomware Using Malicious Logins	https://cybersecuritynews.com/sonicwall-firewalls-akira-ransomware/
New Botnet Loader-as-a-Service Exploiting Routers and IoT Devices to Deploy Mirai Payloads	https://cybersecuritynews.com/new-botnet-loader-as-a-service-exploiting-routers/
Malware Operators Collaborate With Covert North Korean IT Workers to Attack Corporate Organizations	https://cybersecuritynews.com/malware-operators-collaborate-with-covert-north-korean-it-workers/
Hackers use Weaponized Microsoft Teams Installer to Compromise Systems With Oyster Malware	https://cybersecuritynews.com/weaponized-microsoft-teams-installer/

Sneaky, Malicious MCP Server Exfiltrates Secrets via BCC	**https://www.darkreading.com/application-security/malicious-mcp-server-exfiltrates-secrets-bcc**
SonicWall SSL VPN Attacks Escalate, Bypassing MFA	**https://www.infosecurity-magazine.com/news/sonicwall-ssl-vpn-attacks-escalate/**
Hackers Trick Users into Download Weaponized Microsoft Teams to Gain Remote Access	**https://cybersecuritynews.com/weaponized-microsoft-teams/**
SVG Security Analysis Toolkit to Detect Malicious Scripts Hidden in SVG Files	**https://cybersecuritynews.com/svg-security-analysis-toolkit/**
New Malware-as-a-Service Olymp Loader Promises Defender-Bypass With Automatic Certificate Signing	**https://cybersecuritynews.com/new-malware-as-a-service-olymp-loader/**
Threat Actors Weaponizing Facebook and Google Ads as Financial Platforms to Steal Sensitive Data	**https://cybersecuritynews.com/threat-actors-weaponizing-facebook-and-google-ads/**
Threat Actors Leveraging Dynamic DNS Providers to Use for Malicious Purposes	**https://cybersecuritynews.com/threat-actors-leveraging-dynamic-dns-providers/**

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/