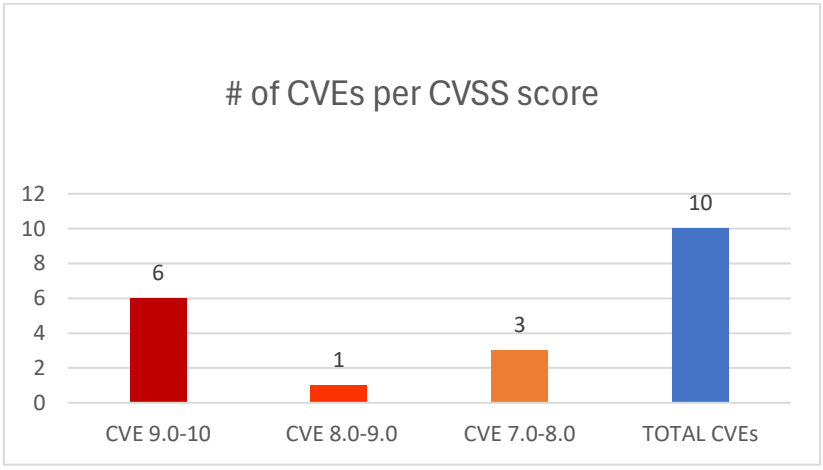
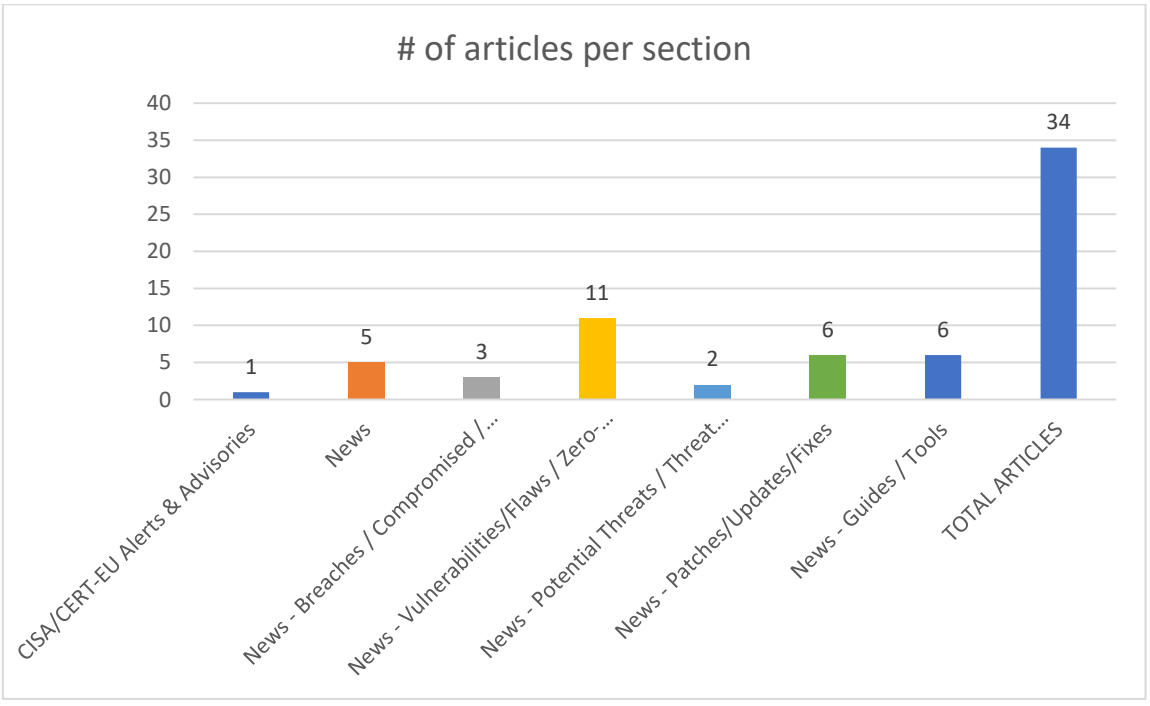
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 18/10/2025 - 21/10/2025





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-2025-62645	**9.9**	The Restaurant Brands International (RBI) assistant platform	Incorrect Privilege Assignment		https://archive.today/fMYQp MITRE https://bobdahacker.com/blog/rbi-hacked-drive-thrus/ MITRE https://web.archive.org/web/20250906134240/https:/bobdahacker.com/blog/rbi-hacked-drive-thrus MITRE https://www.malwarebytes.com/blog/news/2025/09/pop-eyes-tim-hortons-burger-king-platforms-have-catastrophic-vulnerabilities-say-hackers MITRE https://www.yahoo.com/news/articles/burger-king-hacked-attackers-impressed-124154038.html
https://nvd.nist.gov/vuln/detail/CVE-2017-20206	**9.8**	The Appointments plugin for WordPress	Deserialization of Untrusted Data	up to, and including, 2.2.1	https://plugins.trac.wordpress.org/changeset/1733186/appointments Wordfence https://www.wordfence.com/blog/2017/10/3-zero-day-plugin-vulnerabilities-exploited-wild/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/7e8f230e-3f96-4efd-806d-72725b960303?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2017-20207	**9.8**	The Flickr Gallery plugin for WordPress	Deserialization of Untrusted Data	up to, and including, 1.5.2	https://plugins.trac.wordpress.org/changeset/1737576/flickr-gallery Wordfence https://www.wordfence.com/blog/2017/10/3-zero-day-plugin-vulnerabilities-exploited-wild/ Wordfence

					https://www.wordfence.com/threat-intel/vulnerabilities/id/b52ae51d-7b9a-4047-82bf-723ea87d2375?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2017-20208	**9.8**	The RegistrationMagic – Custom Registration Forms, User Registration, Payment, and User Login plugin for WordPress	Deserialization of Untrusted Data	up to 3.7.9.3 (exclusive)	https://plugins.trac.wordpress.org/changeset/1733274/custom-registration-form-builder-with-submission-manager Wordfence https://www.wordfence.com/blog/2017/10/3-zero-day-plugin-vulnerabilities-exploited-wild/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/c2b79193-f8fc-4ea2-8973-fe292cfb926b?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-11948	**9.8**	Document Management System developed by Excellent Infotek	Unrestricted Upload of File with Dangerous Type		https://www.twcert.org.tw/en/cp-139-10453-43e63-2.html TWCERT/CC https://www.twcert.org.tw/tw/cp-132-10452-72cb6-1.html
https://nvd.nist.gov/vuln/detail/CVE-2025-61932	**9.8**	Lanscope Endpoint Manager (On-Premises) (Client program (MR) and Detection agent (DA))	Improper Verification of Source of a Communication Channel		https://jvn.jp/en/jp/JVN86318557/ JPCERT/CC https://www.motex.co.jp/news/notice/2025/release251020/
https://nvd.nist.gov/vuln/detail/CVE-2025-62577	**8.8**	ETERNUS SF provided by Fsas Technologies Inc.	Incorrect Default Permissions		https://jvn.jp/en/jp/JVN44266462/ JPCERT/CC https://www.fsastech.com/ja-jp/resources/security/2025/1020.html JPCERT/CC https://www.fujitsu.com/global/support/products/computing/storage/20251020/index.html
https://nvd.nist.gov/vuln/detail/CVE-2025-11691	**7.5**	The PPOM – Product Addons & Custom Fields for WooCommerce	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to, and including, 33.0.15	https://plugins.trac.wordpress.org/browser/woocommerce-product-addon/trunk/classes/ppom.class.php#L337 Wordfence

		plugin for Word-Press			https://plugins.trac.wordpress.org/chang-eset?sfp_email=&sfph_mail=&re-poname=&old=3379431%40woocommerce-product-ad-don&new=3379431%40woocommerce-product-ad-don&sfp_email=&sfph_mail= Wordfence https://www.wordfence.com/threat-intel/vulnerabili-ties/id/eefcc290-b7f7-4cf0-9ccc-db4c883d6426?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-11517	**7.5**	The Event Tickets and Registration plugin for Word-Press	Authorization Bypass Through User-Controlled Key	up to, and including, 5.26.5	https://plugins.trac.wordpress.org/chang-eset/3378214/event-tickets/tags/5.26.6/src/Tickets/Com-merce/Gateways/Free/REST/Order_Endpoint.php Word-fence https://www.wordfence.com/threat-intel/vulnerabili-ties/id/21cd8cb8-2a29-4b66-ab7a-8d8b2f85e2e0?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2020-36853	**7.2**	The 10WebMap-Builder plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 1.0.63	https://plugins.trac.wordpress.org/changeset/2251882/wd-google-maps Wordfence https://www.wordfence.com/blog/2020/02/site-takeover-campaign-exploits-multiple-zero-day-vulnerabilities/ Word-fence https://www.wordfence.com/threat-intel/vulnerabili-ties/id/7c1c24cc-9388-4d91-8dc6-c67d3420cc94?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 Adds Five Known Exploited Vulnerabilities to Catalog	▪ **CVE-2022-48503 Apple Multiple Products Unspecified Vulnerability** ▪ **CVE-2025-2746 Kentico Xperience Staging Sync Server Digest Password Authentication Bypass Vulnerability** ▪ **CVE-2025-2747 Kentico Xperience Staging Sync Server None Password Type Authentication Bypass Vulnerability** ▪ **CVE-2025-33073 Microsoft Windows SMB Client Improper Access Control Vulnerability** ▪ **CVE-2025-61884 Oracle E-Business Suite Server-Side Request Forgery (SSRF) Vulnerability**	**https://www.cisa.gov/news-events/alerts/2025/10/20/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
Authorities Dismantle Cybercrime-as-a-Service Platform, Seize 40,000 Active SIM Cards	**https://cybersecuritynews.com/cybercrime-as-a-service-platform-dismantled/**
Microsoft Revokes 200+ Fake Certificates Used in Teams Malware Attack	**https://www.infosecurity-magazine.com/news/microsoft-revokes-200-fake/**
AI-Driven Social Engineering Top Cyber Threat for 2026, ISACA Survey Reveals	**https://www.infosecurity-magazine.com/news/ai-social-engineering-top-cyber/**
ColdRiver Drops Fresh Malware on Targets	**https://www.darkreading.com/cyberattacks-data-breaches/coldriver-drops-fresh-malware-targets**
Five New Exploited Bugs Land in CISA's Catalog — Oracle and Microsoft Among Targets	**https://thehackernews.com/2025/10/five-new-exploited-bugs-land-in-cisas.html**

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
Volkswagen Allegedly Hit by Ransomware Attack as 8Base Claims Sensitive Data Theft	https://cybersecuritynews.com/volkswagen-ransomware-attack/
American Airlines Subsidiary Envoy Compromised in Oracle Hacking Campaign	https://cybersecuritynews.com/envoy-compromised-oracle-campaign/
Threat Brief: Nation-State Actor Steals F5 Source Code and Undisclosed Vulnerabilities	https://unit42.paloaltonetworks.com/nation-state-threat-actor-steals-f5-source-code/?&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
ZYXEL Authorization Bypass Vulnerability Let Attackers View and Download System Configuration	https://cybersecuritynews.com/zyxel-devices-exposed/
Critical ASP.NET Vulnerability Allows Attacker To Bypass Security Feature Remotely	https://cybersecuritynews.com/critical-asp-net-vulnerability/
CISA Warns of Windows SMB Vulnerability Actively Exploited in Attacks	https://cybersecuritynews.com/windows-smb-vulnerability-exploited/
71,000+ WatchGuard Devices Vulnerable to Remote Code Execution Attacks	https://cybersecuritynews.com/watchguard-devices-rce-attack/
Dolby Digital Plus 0-Click Vulnerability Enables RCE Attack via Malicious Audio on Android	https://cybersecuritynews.com/dolby-digital-plus-0-click-vulnerability/
New DefenderWrite Tool Let Attackers Inject Malicious DLLs into AV Executable Folders	https://cybersecuritynews.com/defenderwrite-tool/
PoC Exploit Released for Linux-PAM Vulnerability Allowing Root Privilege Escalation	https://cybersecuritynews.com/poc-exploit-linux-pam-vulnerability/
WatchGuard VPN Vulnerability Let Remote Attacker Execute Arbitrary Code	https://cybersecuritynews.com/watchguard-vpn-vulnerability/
PoC Exploit for 7-Zip Vulnerabilities that Allows Remote Code Execution	https://cybersecuritynews.com/poc-exploit-7-zip-vulnerabilities/

Critical Zimbra SSRF Vulnerability Let Attackers Access Sensitive Data	**https://cybersecuritynews.com/zimbra-ssrf-vulnerability/**
Salt Typhoon Uses Citrix Flaw in Global Cyber-Attack	**https://www.infosecurity-magazine.com/news/salt-typhoon-citrix-flaw-cyber/**

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
AWS Declares Major Outage Resolved After Nearly 24 Hours of Disruption	**https://cybersecuritynews.com/aws-outage-resolved/**
AWS Outage Impacts Amazon, Snapchat, Prime Video, Canva and More – Update	**https://cybersecuritynews.com/aws-outage/**
PoC Exploit Released for Windows Server Update Services Remote Code Execution Vulnerability	**https://cybersecuritynews.com/poc-wsus-rce-vulnerability/**
Windows 11 24H2/25H2 Update Blocks Mouse and Keyboard in Recovery Mode	**https://cybersecuritynews.com/windows-11-24h2-25h2-update-blocks-recovery/**
Microsoft fixes highest-severity ASP.NET Core flaw ever	**https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-highest-severity-aspnet-core-flaw-ever/**
ConnectWise Patches Critical Flaw in Automate RMM Tool	**https://www.securityweek.com/connectwise-patches-critical-flaw-in-automate-rmm-tool/**

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 Attacking Remote Desktop Protocol Services With 30,000+ New IP Addresses Daily	**https://cybersecuritynews.com/rdp-services-under-attack/**
New Phishing Attack Leverages Azure Blob Storage to Impersonate Microsoft	**https://cybersecuritynews.com/phishing-attack-leverages-azure-blob-storage/**

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/