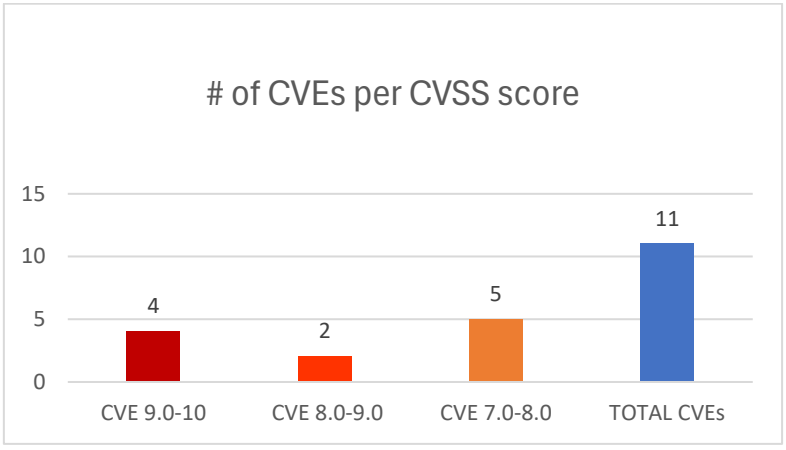
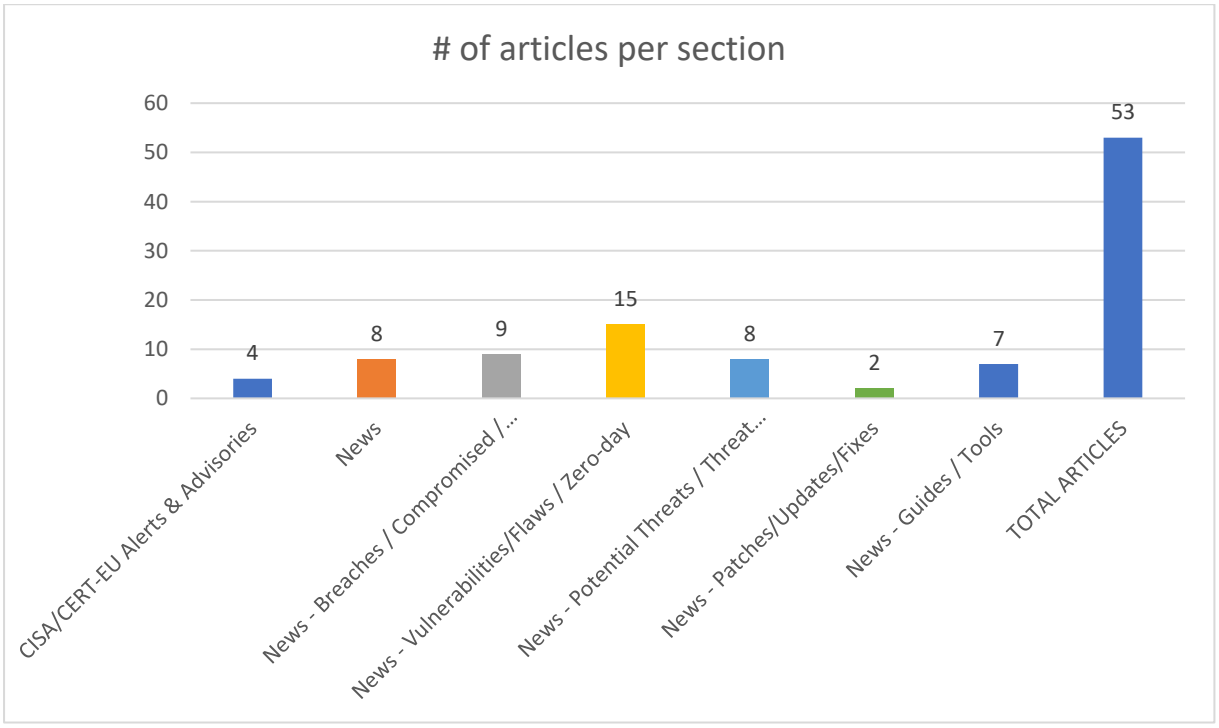
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 28/10/2025 - 31/10/2025





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-2025-36386	9,8	IBM Maximo Application Suite	Authentication Bypass by Primary Weakness	9.0.0 through 9.0.15 and 9.1.0 through 9.1.4	https://www.ibm.com/support/pages/node/7249416
https://nvd.nist.gov/vuln/detail/CVE-2025-12380	9,8	Starting with Firefox 142	use-after-free	< 144.0.2	https://bugzilla.mozilla.org/show_bug.cgi?id=1993113 Mozilla Corporation https://www.mozilla.org/security/advisories/mfsa2025-86/
https://nvd.nist.gov/vuln/detail/CVE-2025-61128	9,1	WAVLINK QUANTUM	arbitrary code execution	D3G/WL-WN530HG3 firmware M30HG3_V240730	https://gist.github.com/shinobu-alpha/6dd5ad7f83c16360f6564db0bc121e99
https://nvd.nist.gov/vuln/detail/CVE-2025-61043	9,1	Monkey's Audio	improper handling of the length of the input	11.31	https://tzh00203.notion.site/Monkey-s-Audio-Out-of-Bounds-Read-Vulnerability-Report-version-11-31-249b5c52018a80739852d0d9660994c9?source=copy_link
https://nvd.nist.gov/vuln/detail/CVE-2025-56399	8,8	alexusmai laravel-file-manager		3.3.1 and before	http://laravel-file-manager.com MITRE https://github.com/Theethat-Thamwasin/CVE-2025-56399
https://nvd.nist.gov/vuln/detail/CVE-2025-62777	8,8	MZK-DP300N	Use of Hard-coded Credentials	1.07 and earlier	https://jvn.jp/en/jp/JVN00021602/ JPCERT/CC https://www.planex.co.jp/products/mzk-dp300n/
https://nvd.nist.gov/vuln/detail/CVE-2025-53855	7,8	XML parser functionality of GCC Productions Inc. Fade	Out-of-bounds Write	4.2.0	https://talosintelligence.com/vulnerability_reports/TALOS-2025-2250
https://nvd.nist.gov/vuln/detail/CVE-2025-10145	7,7	The Auto Featured Image (Auto Post Thumbnail)	Server-Side Request Forgery (SSRF)	up to, and including, 4.1.7	https://plugins.trac.wordpress.org/browser/auto-post-thumbnail/tags/4.1.7/includes/class-apt.php#L821 Wordfence

		plugin for WordPress			https://www.wordfence.com/threat-intel/vulnerabilities/id/93acfae6-470b-4637-b76b-e1162b80253f?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-54604	7,5	Bitcoin Core	Uncontrolled Resource Consumption	through 29.0	https://bitcoincore.org/en/2025/10/24/disclose-cve-2025-54604/ MITRE https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures MITRE https://github.com/bitcoin/bitcoin/releases
https://nvd.nist.gov/vuln/detail/CVE-2025-61104	7,5	FRRouting/frr	NULL pointer dereference	from v4.0 through v10.4.1	https://github.com/FRRouting/frr/issues/19471 MITRE https://github.com/FRRouting/frr/pull/19480 MITRE https://github.com/FRRouting/frr/pull/19480/commits/fdd957408605d4a1766225630aafc7e6b7c3daf3 MITRE https://github.com/s1awwhy/BugList/blob/main/CVE-2025-61104.md
https://nvd.nist.gov/vuln/detail/CVE-2025-11735	7,5	The HUSKY – Products Filter Professional for WooCommerce plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to, and including, 1.3.7.1	https://plugins.trac.wordpress.org/browser/woocommerce-products-filter/trunk/ext/by_text_2/index.php#L164 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/ebaec880-0d1c-4725-a746-530f48821279?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 Two Known Exploited Vulnerabilities to Catalog	▪ **CVE-2025-24893 XWiki Platform Eval Injection Vulnerability** ▪ **CVE-2025-41244 Broadcom VMware Aria Operations and VMware Tools Privilege Defined with Unsafe Actions Vulnerability**	**https://www.cisa.gov/news-events/alerts/2025/10/30/cisa-adds-two-known-exploited-vulnerabilities-catalog**
CISA Releases Two Industrial Control Systems Advisories	▪ ICSA-25-303-01 International Standards Organization ISO 15118-2 ▪ ICSA-25-303-02 Hitachi Energy TropOS	https://www.cisa.gov/news-events/alerts/2025/10/30/cisa-releases-two-industrial-control-systems-advisories
New Guidance Released on Microsoft Exchange Server Security Best Practices		https://www.cisa.gov/news-events/alerts/2025/10/30/new-guidance-released-microsoft-exchange-server-security-best-practices
ED 26-01: Mitigate Vulnerabilities in F5 Devices		https://www.cisa.gov/news-events/directives/ed-26-01-mitigate-vulnerabilities-f5-devices

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
Russian Hackers Target Ukrainian Organizations Using Stealthy Living-Off-the-Land Tactics	**https://thehackernews.com/2025/10/russian-hackers-target-ukrainian.html**
Microsoft Security Change for Azure VMs Creates Pitfalls	**https://www.darkreading.com/cloud-security/microsoft-security-change-azure-vms-creates-pitfalls**
LotL Attack Hides Malware in Windows Native AI Stack	**https://www.darkreading.com/vulnerabilities-threats/lotl-attack-malware-windows-native-ai-stack**
Ex-L3Harris exec guilty of selling cyber exploits to Russian broker	**https://www.bleepingcomputer.com/news/security/ex-l3harris-exec-guilty-of-selling-cyber-exploits-to-russian-broker/**
Open Source “b3” Benchmark to Boost LLM Security for Agents	**https://www.infosecurity-magazine.com/news/open-source-b3-benchmark-security/**

Chrome to Make HTTPS Mandatory by Default in 2026	https://www.infosecurity-magazine.com/news/chrome-https-mandatory-2026/
New Agent-Aware Cloaking Leverages OpenAI ChatGPT Atlas Browser to Deliver Fake Content	https://cybersecuritynews.com/agent-aware-cloaking-chatgpt-atlas/
Cyberpunks mess with Canada's water, energy, and farm systems	https://www.theregister.com/2025/10/30/hacktivists_canadian_ics_systems/?&web_view=true

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
Dentsu Subsidiary Breached, Employee Data Stolen	https://www.darkreading.com/cyberattacks-data-breaches/dentsu-subsidiary-breached-employee-data-stolen
WordPress security plugin exposes private data to site subscribers	https://www.bleepingcomputer.com/news/security/wordpress-security-plugin-exposes-private-data-to-site-subscribers/
Proton Claims 300 Million Records Compromised So Far This Year	https://www.infosecurity-magazine.com/news/proton-300-million-records/
AzureHound Penetration Testing Tool Weaponized by Threat Actors to Enumerate Azure and Entra ID	https://cybersecuritynews.com/azurehound-enumerate-azure-entra-id/
Historic Great Firewall Breach – 500GB+ Censorship Data Exposed	https://cybersecuritynews.com/historic-great-firewall-breach/
New Lampion Stealer Uses ClickFix Attack to Silently Steal Login Credentials	https://cybersecuritynews.com/new-lampion-stealer-uses-clickfix-attack/
Tata Motors Data Leak – 70+ TB of Sensitive Info and Test Drive Data Exposed via AWS Keys	https://cybersecuritynews.com/tata-motors-data-leak/
EY Data Leak – Massive 4TB SQL Server Backup Exposed Publicly on Microsoft Azure	https://cybersecuritynews.com/ey-data-leak/
WordPress Plugin Vulnerability Exposes 7 Million Sites to XSS Attack	https://cybersecuritynews.com/wordpress-litespeed-cache-plugin-vulnerability/

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
CISA Flags VMware Zero-Day Exploited by China-Linked Hackers in Active Attacks	https://thehackernews.com/2025/10/cisa-flags-vmware-zero-day-exploited-by.html
New "Brash" Exploit Crashes Chromium Browsers Instantly with a Single Malicious URL	https://thehackernews.com/2025/10/new-brash-exploit-crashes-chromium.html

Active Exploits Hit Dassault and XWiki — CISA Confirms Critical Flaws Under Attack	https://thehackernews.com/2025/10/active-exploits-hit-dassault-and-xwiki.html
Critical Claroty Authentication Bypass Flaw Opened OT to Attack	https://www.darkreading.com/ics-ot-security/claroty-patches-authentication-bypass-flaw
Critical Flaws Found in Elementor King Addons Affect 10,000 Sites	https://www.infosecurity-magazine.com/news/critical-flaws-elementor-king/
CISA Warns of VMware Tools and Aria Operations 0-Day Vulnerability Exploited in Attacks	https://cybersecuritynews.com/vmware-tools-and-aria-operations-0-day/
RediShell RCE Vulnerability Exposes 8,500+ Redis Instances to Code Execution Attacks	https://cybersecuritynews.com/redishell-rce-vulnerability-exposes-8500-redis/
Multiple Jenkins Vulnerability SAML Authentication Bypass And MCP Server Plugin Permissions	https://cybersecuritynews.com/multiple-jenkins-vulnerability/
Critical Vulnerability in Chromium's Blink Let Attackers Crash Chromium-based Browsers Within Seconds	https://cybersecuritynews.com/chromium-blink-vulnerability/
Docker Compose Vulnerability Allow Attacks To Overwrite Arbitrary Files	https://cybersecuritynews.com/docker-compose-vulnerability/
Microsoft Details ASP.NET Vulnerability That Enables Attackers To Smuggle HTTP Requests	https://cybersecuritynews.com/microsoft-details-asp-net-vulnerability/
Magento Input Validation Vulnerability Exploited In Wild To Hijack Session And Execute Malicious Codes	https://cybersecuritynews.com/magento-input-validation-vulnerability/
Microsoft DNS Outage Disrupts Azure and Microsoft 365 Services Worldwide	https://cybersecuritynews.com/microsoft-dns-outage/
New TEE.fail Attack Breaks Trusted Environments to Exfiltrate Secrets from Intel and AMD DDR5 Environments	https://cybersecuritynews.com/new-tee-fail-attack-breaks-trusted-environments/
Thousands of Exchange Servers in Germany Still Running with Out-of-Support Versions	https://cybersecuritynews.com/germany-exchange-servers-out-of-support/

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
WhatsApp Introduces Passkey Encryption for Enhanced Chat Message Backup Security	https://cybersecuritynews.com/whatsapp-passkey-encryption-for-chat/
Chrome 142 Released With Fix for 20 Vulnerabilities that Allow Malicious Code Execution	https://cybersecuritynews.com/chrome-142-released-fix-20-vulnerabilities/

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
PHP Servers and IoT Devices Face Growing Cyber-Attack Risks	https://www.infosecurity-magazine.com/news/php-servers-and-iot-devices-cyber/
Npm Malware Uses Invisible Dependencies to Infect Dozens of Packages	https://www.infosecurity-magazine.com/news/npm-malware-invisible-dependencies/
Threat Actors Utilize AdaptixC2 for Malicious Payload Delivery	https://www.infosecurity-magazine.com/news/adaptixc2-malicious-payload/
Threat Actors Using Multilingual ZIP File to Attack Financial and Government Organizations	https://cybersecuritynews.com/threat-actors-using-multilingual-zip-file/
New Windows-Based Airstalk Malware Employs Multi-Threaded C2 Communication to Steal Logins	https://cybersecuritynews.com/new-windows-based-airstalk-malware/
700+ Malicious Android Apps Abusing NFC Relay to Exfiltrate Banking Login Credentials	https://cybersecuritynews.com/700-malicious-android-apps-abusing-nfc-relay/
New Malware Targeting WooCommerce Sites with Malicious Plugins Steals Credit Card Data	https://cybersecuritynews.com/new-malware-targeting-woocommerce-sites/
12 Malicious Extension in VSCode Marketplace Steal Source Code and Exfiltrate Login Credentials	https://cybersecuritynews.com/12-malicious-extension-in-vscode-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/

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/