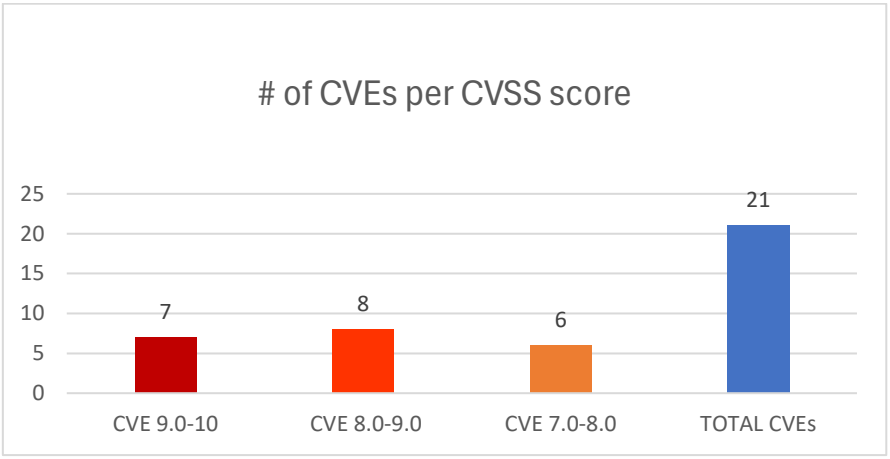
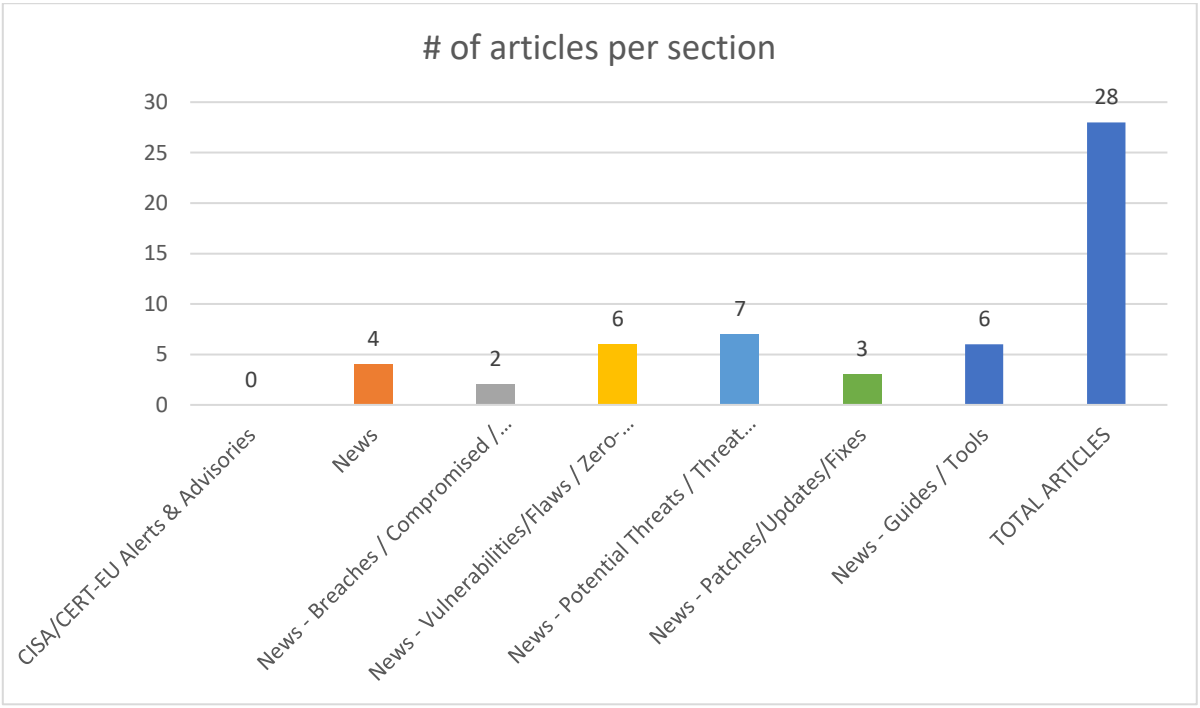
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 11/10/2025 - 14/10/2025





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-2025-6439	**9.8**	The WooCommerce Designer Pro plugin for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	up to, and including, 1.9.26	https://codecanyon.net/item/woocommerce-designer-pro-cmyk-card-flyer/22027731 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/407a0bc3-2775-4a34-9817-924bf94a4f94?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-6553	**9.8**	The Ovatheme Events Manager plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 1.8.5	https://themeforest.net/item/em4u-event-management-multipurpose-wordpress-theme/20846579 Wordfence https://themeforest.net/item/em4u-event-management-multipurpose-wordpress-theme/20846579#item-description__change_log Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/808392a9-dbac-4896-8677-6ddc1213d80d?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-11533	**9.8**	The WP Freeio plugin for WordPress	Improper Privilege Management	up to, and including, 1.2.21	https://themeforest.net/item/freeio-freelance-marketplace-wordpress-theme/42045416 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/0db85f84-04e9-42eb-a16b-96554fbfd186?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-42937	**9.8**	SAP Print Service (SAPSprint)	Path Traversal: '.../...//'		https://me.sap.com/notes/3630595 SAP SE https://url.sap/sapsecuritypatchday
https://nvd.nist.gov/vuln/detail/CVE-2025-6919	**9.6**	Cats Information Technology Software Development Technologies Aykome License Tracking System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	before Version dated 06.10.2025	https://www.usom.gov.tr/bildirim/tr-25-0332

https://nvd.nist.gov/vuln/detail/CVE-2025-37729	**9.1**	Elastic Cloud Enterprise (ECE)	Improper Neutralization of Special Elements Used in a Template Engine		https://discuss.elastic.co/t/elastic-cloud-enterprise-ece-3-8-2-and-4-0-2-security-update-esa-2025-21/382641
https://nvd.nist.gov/vuln/detail/CVE-2025-42910	**9.0**	SAP Supplier Relationship Management	Unrestricted Upload of File with Dangerous Type		https://me.sap.com/notes/3647332 SAP SE https://url.sap/sapsecuritypatchday
https://nvd.nist.gov/vuln/detail/CVE-2025-8593	**8.8**	The GSheetConnector For Gravity Forms plugin for WordPress	Missing Authorization	less than, or equal to, 1.3.27	https://plugins.trac.wordpress.org/browser/gsheetconnector-gravity-forms/tags/1.3.23/includes/class-gravityform-gs-service.php#L128 Wordfence https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3354113%40gsheetconnector-gravity-forms&new=3354113%40gsheetconnector-gravity-forms&sfp_email=&sfph_mail= Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/c7266ce6-2853-4c5d-9e36-8c5b7418b072?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-11586	**8.8**	Tenda AC7	Stack-based Buffer Overflow	15.03.06.44	https://github.com/noahze01/IoT-vulnerable/blob/main/Tenda/AC7/set-NotUpgrade.md VulDB https://github.com/noahze01/IoT-vulnerable/blob/main/Tenda/AC7/set-NotUpgrade.md#exploit VulDB https://vuldb.com/?ctiid.327908 VulDB https://vuldb.com/?id.327908 VulDB https://vuldb.com/?submit.671597 VulDB https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-11653	**8.8**	UTT HiPER 2620G	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	up to 3.1.4	https://github.com/ashin9/CVE/issues/2 VulDB https://vuldb.com/?ctiid.328070 VulDB https://vuldb.com/?id.328070 VulDB https://vuldb.com/?submit.665712
https://nvd.nist.gov/vuln/detail/CVE-2025-59889	**8.6**	Eaton IPP	Uncontrolled Search Path Element		https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2025-1009.pdf

https://nvd.nist.gov/vuln/detail/CVE-2025-61688	**8.6**	Omni manages Kubernetes	Exposure of Sensitive Information to an Unauthorized Actor	Prior to 1.1.5 and 1.0.2	https://github.com/siderolabs/omni/security/advisories/GHSA-77r9-w39m-9xh5
https://nvd.nist.gov/vuln/detail/CVE-2025-58299	**8.4**	storage management module	Use After Free		https://consumer.huawei.com/en/support/bulletin/2025/10/
https://nvd.nist.gov/vuln/detail/CVE-2025-36087	**8.1**	IBM Security Verify Access	Use of Hard-coded Credentials	10.0.0 through 10.0.9, 11.0.0	https://www.ibm.com/support/pages/node/7247753
https://nvd.nist.gov/vuln/detail/CVE-2025-11695	**8.0**	MongoDB Rust Driver	Improper Certificate Validation	prior to v3.2.5	https://jira.mongodb.org/browse/RUST-2264
https://nvd.nist.gov/vuln/detail/CVE-2025-11622	**7.8**	Ivanti Endpoint Manager	Deserialization of Untrusted Data		https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-EPM-October-2025
https://nvd.nist.gov/vuln/detail/CVE-2025-61884	**7.5**	Oracle Configurator product of Oracle E-Business Suite	unauthorized access	12.2.3-12.2.14	https://www.oracle.com/security-alerts/alert-cve-2025-61884.html
https://nvd.nist.gov/vuln/detail/CVE-2025-62162	**7.5**	cel-rust	Improper Input Validation	0.10.0 and prior to version 0.11.4	https://github.com/cel-rust/cel-rust/releases/tag/cel-v0.11.4 GitHub, Inc. https://github.com/cel-rust/cel-rust/security/advisories/GHSA-wxwx-9fh7-5mrw
https://nvd.nist.gov/vuln/detail/CVE-2025-62170	**7.5**	rAthena	Use After Free		https://github.com/rathena/rathena/commit/af2f3ba33fc03dc6dd510f8cfe84cd9185af748d GitHub, Inc. https://github.com/rathena/rathena/security/advisories/GHSA-9mj9-8vgv-r92j

https://nvd.nist.gov/vuln/detail/CVE-2025-7707	**7.1**	The llama_index library	Insecure Temporary File	0.12.33	https://github.com/run-llama/llama_index/commit/98816394d57c7f53f847ed7b60725e69d0e7aae4 huntr.dev https://huntr.com/bounties/3fe2c8ab-6727-4aef-a0ef-4d2818e48803
https://nvd.nist.gov/vuln/detail/CVE-2025-11649	**7.0**	Tomofun Furbo 360 and Furbo Mini	Credentials Management Errors	Furbo 360 up to FB0035_FW_036 and Furbo Mini up to MC0020_FW_074	https://github.com/dead1nfluence/Furbo-Advisories/blob/main/Hard-coded-Password.md VulDB https://vuldb.com/?ctiid.328060 VulDB https://vuldb.com/?id.328060 VulDB https://vuldb.com/?submit.662769

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

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-Russian Hacktivist Attacking OT/ICS Devices to Steal Login Credentials	https://cybersecuritynews.com/pro-russian-hacktivist-attacking-ot-ics-devices/
Hackers Can Bypass OpenAI Guardrails Using a Simple Prompt Injection Technique	https://cybersecuritynews.com/openai-guardrails-bypassed/
North Korean Hackers Attacking Developers with 338 Malicious npm Packages	https://cybersecuritynews.com/north-korean-hackers-attacking-developers/
UK Firms Lose Average of £2.9m to AI Risk	https://www.infosecurity-magazine.com/news/uk-firms-lose-average-29m-ai-risk/

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
Experts Warn of Widespread SonicWall VPN Compromise Impacting Over 100 Accounts	https://thehackernews.com/2025/10/experts-warn-of-widespread-sonicwall.html
178,000+ Invoices Expose Customer Data from Invoicely Platform	https://gbhackers.com/customer-data/?&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
New Oracle E-Business Suite Bug Could Let Hackers Access Data Without Login	https://thehackernews.com/2025/10/new-oracle-e-business-suite-bug-could.html
Another remotely exploitable Oracle EBS vulnerability requires your attention (CVE-2025-61884)	https://www.helpnetsecurity.com/2025/10/12/another-remotely-exploitable-oracle-ebs-vulnerability-requires-your-attention-cve-2025-61884/
CVE-2025-11371: Unpatched zero-day in Gladinet CentreStack, Triofox under attack	https://securityaffairs.com/183259/hacking/cve-2025-11371-unpatched-zero-day-in-gladinet-centrestack-triofox-under-attack.html
Happy DOM Vulnerability Exposes 2.7 Million Users To Remote Code Execution Attacks	https://cybersecuritynews.com/happy-dom-vulnerability/
Elastic Cloud Enterprise Vulnerability Let Attackers Execute Malicious Commands	https://cybersecuritynews.com/elastic-cloud-enterprise-vulnerability/
Axis Communications Vulnerability Exposes Azure Storage Account Credentials	https://cybersecuritynews.com/axis-communications-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 Fixes Long-standing Windows 11 ‘Update and Shut down’ Bug	https://cybersecuritynews.com/windows-11-update-and-shut-down-bug/
Ivanti Patches 13 Vulnerabilities in Endpoint Manager Allowing Remote Code Execution	https://cybersecuritynews.com/ivanti-patches-13-vulnerabilities/
Linux Kernel 6.18-rc1 Released With Extensive Updates Following a Steady Merge Window	https://cybersecuritynews.com/linux-kernel-6-18-rc1-released/

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 Turn Velociraptor DFIR Tool Into Weapon in LockBit Ransomware Attacks	https://thehackernews.com/2025/10/hackers-turn-velociraptor-dfir-tool.html
RealBlindingEDR Tool That Permanently Turns Off AV/EDR Using Kernel Callbacks	https://cybersecuritynews.com/realblindingedr-tool/
Hackers Can Inject Malicious Code into Antivirus to Create a Backdoor	https://cybersecuritynews.com/malicious-code-into-antivirus/
Microsoft Defender Vulnerabilities Allow Attackers to Bypass Authentication and Upload Malicious Files	https://cybersecuritynews.com/microsoft-defender-authentication-bypass/
Hackers Attacking Remote Desktop Protocol Services from 100,000+ IP Addresses	https://cybersecuritynews.com/hackers-attacking-rdp-services/
New Stealit Malware Attacking Windows Systems Abuses Node.js Extensions	https://cybersecuritynews.com/new-stealit-malware-attacking-windows-systems/
New WhatsApp Worm Attacks Users with Banking Malware to Users Login Credentials	https://cybersecuritynews.com/new-whatsapp-worm-attacks-users-with-banking-malware/

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/