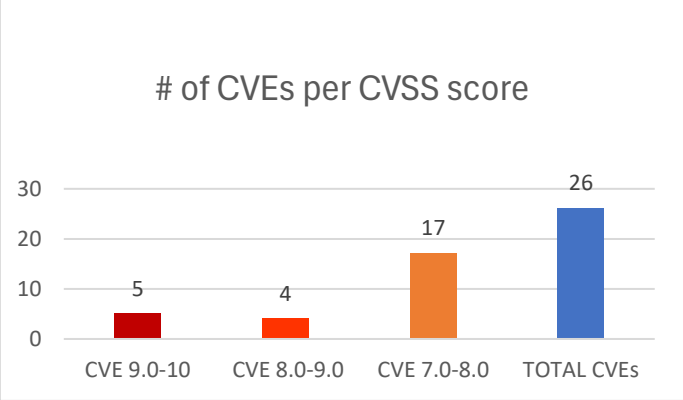
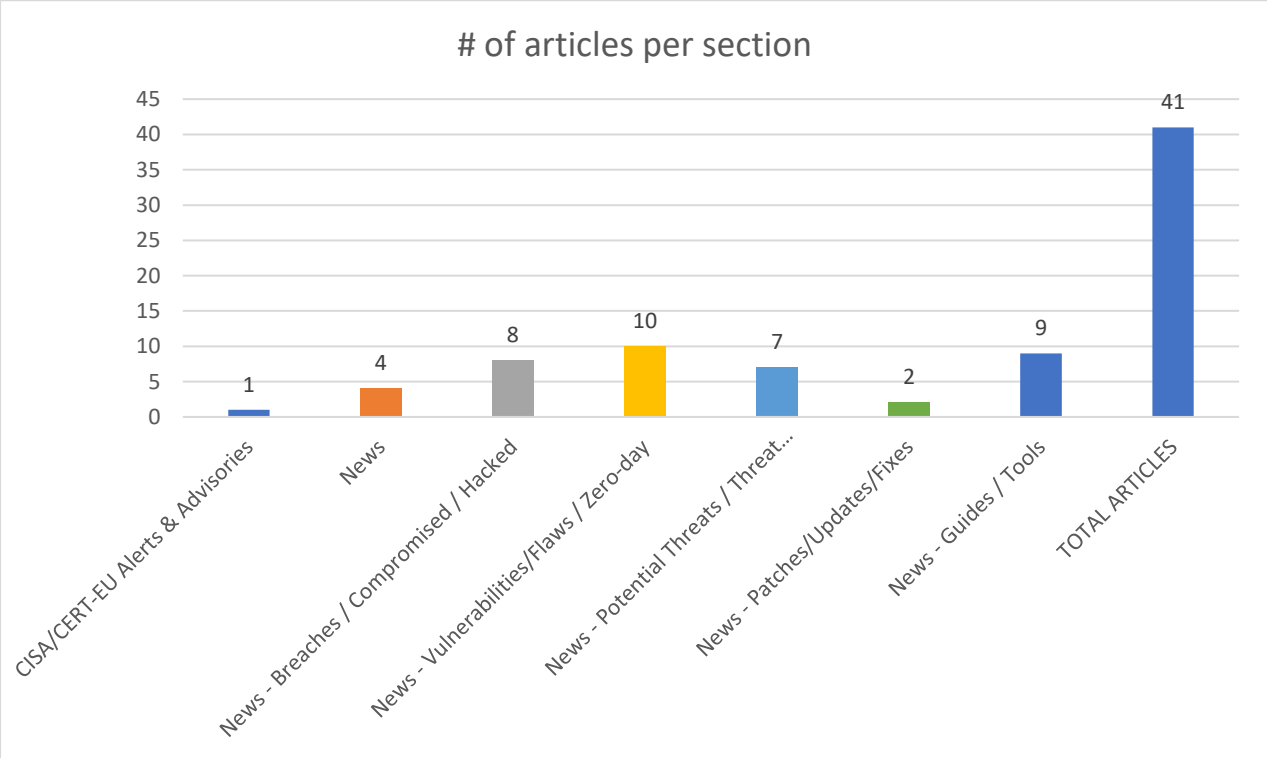
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 29/11/2025 - 02/12/2025





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-2025-13615	9,8	The StreamTube Core plugin for WordPress	Authorization Bypass Through User-Controlled Key	up to, and including, 4.78	https://themeforest.net/item/streamtube-responsive-video-word-press-theme/33821786 Wordfence https://www.wordfence.com/threat-intel/vulnerabili-ties/id/b812a0d7-99a1-4f61-b78a-78cea6a2ada1?source=cve
https://nvd.nist.gov/vuln/de-tail/CVE-2025-66401	9,8	MCP Watch	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	In 0.1.2 and earlier	https://github.com/kapilduraphe/mcp-watch/com-mit/e7da78c5b4b960f8b66c254059ad9ebc544a91a6 GitHub, Inc. https://github.com/kapilduraphe/mcp-watch/security/adviso-ries/GHSA-27m7-ffhq-jqrm
https://nvd.nist.gov/vuln/de-tail/CVE-2025-35028	9,1	the HexStrike AI MCP server	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')		https://github.com/0x4m4/hexstrike-ai/issues/115
https://nvd.nist.gov/vuln/de-tail/CVE-2025-12106	9,1	OpenVPN	Buffer Over-read	2.7_alpha1 through 2.7_rc1	https://community.openvpn.net/Security%20Announcements/CVE-2025-12106 OpenVPN Inc. https://www.mail-archive.com/openvpn-announce@lists.source-forge.net/msg00152.html
https://nvd.nist.gov/vuln/de-tail/CVE-2025-8351	9,0	Avast Antivirus on MacOS	Heap-based Buffer Overflow	from 8.3.70.94 before 8.3.70.98	https://www.gendigital.com/us/en/contact-us/security-advisories/
https://nvd.nist.gov/vuln/detail/CVE-2025-12529	8,8	The Cost Calculator Builder plugin for Word-Press	External Control of File Name or Path	up to, and including, 3.6.3.	https://plugins.trac.wordpress.org/browser/cost-calculator-builder/tags/3.6.1/includes/classes/CCBOrderController.php#L262 Wordfence https://plugins.trac.wordpress.org/browser/cost-calculator-builder/tags/3.6.1/includes/classes/CCBOrderController.php#L513 Wordfence https://www.wordfence.com/threat-intel/vulnerabili-ties/id/4154684d-3f9b-418f-b9d1-a5d22d4d84d3?source=cve
https://nvd.nist.gov/vuln/de-tail/CVE-2025-66300	8,5	Grav is a file-based Web platform	Improper Limitation of a Path-name to a Restricted Direc-tory ('Path Traversal')	Prior to 1.8.0-beta.27	https://github.com/getgrav/grav/com-mit/ed640a13143c4177af013cf001969ed2c5e197ee GitHub, Inc. https://github.com/getgrav/grav/security/advisories/GHSA-p4ww-mcp9-j6f2

https://nvd.nist.gov/vuln/detail/CVE-2025-63533	8,5	Blood Bank Management System	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	1.0	https://drive.google.com/file/d/12yeOXW_sN69QjsQtW0_k9AGqozi1s0di/view?usp=sharing MITRE https://github.com/Shridharshukl/Blood-Bank-Management-System MITRE https://github.com/kiwi865/CVEs/blob/main/CVE-2025-63533.md
https://nvd.nist.gov/vuln/detail/CVE-2025-13516	8,1	The SureMail – SMTP and Email Logs Plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to and including 1.9.0	https://cwe.mitre.org/data/definitions/434.html Wordfence https://plugins.trac.wordpress.org/browser/suremails/trunk/inc/admin/plugin.php#L407 Wordfence https://plugins.trac.wordpress.org/browser/suremails/trunk/inc/emails/handler/uploads.php#L113 Wordfence https://plugins.trac.wordpress.org/browser/suremails/trunk/inc/emails/handler/uploads.php#L231 Wordfence https://plugins.trac.wordpress.org/changeset/3403145/suremails/trunk?contextall=1&old=3389326&old_path=%2Fsuremails%2Ftrunk Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/f3a20047-a325-4d29-a848-7ffa525d0bad?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-64772	7,8	The installer of INZONE Hub	Uncontrolled Search Path Element	1.0.10.3 to 1.0.17.0	https://jvn.jp/en/jp/JVN28247549/ JPCERT/CC https://www.sony.com/electronics/support/others-software/inzone-hub
https://nvd.nist.gov/vuln/detail/CVE-2025-61228	7,8	Shirt Pocket SuperDuper!	Download of Code Without Integrity Check	V.3.10	http://shirt.com MITRE https://shirt-pocket.com/SuperDuper/SuperDuperDescription.html MITRE https://www.shirtpocket.com/blog/index.php/shadedgrey/comments/superduper_security_update_v311/
https://nvd.nist.gov/vuln/detail/CVE-2025-61618	7,5	nr modem	improper input validation		https://www.unisoc.com/en/support/announcement/1995394837938163714
https://nvd.nist.gov/vuln/detail/CVE-2025-59789	7,5	json2pb component in Apache bRPC	Uncontrolled Recursion	< 1.15.0	http://www.openwall.com/lists/oss-security/2025/12/01/1 CVE https://lists.apache.org/thread/ozmcsztcpxn61jxod8jo8q46jo0oc1zx
https://nvd.nist.gov/vuln/detail/CVE-2025-54848	7,5	Modbus TCP and Modbus RTU over TCP functionality of Socomec DIRIS	Missing Authentication for Critical Function	Digiware M-70 1.6.9	https://talosintelligence.com/vulnerability_reports/TALOS-2025-2248

https://nvd.nist.gov/vuln/detail/CVE-2024-56089	7,5	Technitium	Use of Insufficiently Random Values	through v13.2.2	https://github.com/TechnitiumSoftware/DnsServer/blob/master/CHANGELOG.md#version-134 MITRE https://technitium.com/dns/
https://nvd.nist.gov/vuln/detail/CVE-2025-13724	7,5	The VikRentCar Car Rental Management System plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to, and including, 1.4.4	https://plugins.trac.wordpress.org/browser/vikrentcar/tags/1.4.4/admin/views/overv/view.html.php#L195 Wordfence https://plugins.trac.wordpress.org/browser/vikrentcar/trunk/admin/views/overv/view.html.php#L195 Wordfence https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3403439%40vikrentcar&new=3403439%40vikrentcar&sfp_email=&sfph_mail= Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/724a2da0-e4e7-4868-a1ad-fce69a915981?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-13803	7,3	MediaCrush	Improper Neutralization of HTTP Headers for Scripting Syntax	1.0.0/1.0.1.	https://github.com/lakshayyverma/CVE-Discovery/blob/main/mediacrush.md VulDB https://vuldb.com/?ctiid.333813 VulDB https://vuldb.com/?id.333813 VulDB https://vuldb.com/?submit.691857
https://nvd.nist.gov/vuln/detail/CVE-2025-13792	7,3	Qualitor	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	up to 8.20.104/8.24.97	https://vuldb.com/?ctiid.333796 VulDB https://vuldb.com/?id.333796 VulDB https://vuldb.com/?submit.691251 VulDB https://www.qualitor.com.br/official-security-advisory-cve-2025-13792 VulDB https://www.youtube.com/watch?v=hU8YbFc6KpI
https://nvd.nist.gov/vuln/detail/CVE-2025-13788	7,3	Chanjet CRM	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to 20251106	https://github.com/Bellingham-max/CVE/issues/1 VulDB https://vuldb.com/?ctiid.333792 VulDB https://vuldb.com/?id.333792 VulDB https://vuldb.com/?submit.690084
https://nvd.nist.gov/vuln/detail/CVE-2025-13786	7,3	taosir WTCMS	Improper Control of Generation of Code ('Code Injection')	up to 01a5f68a3dfc2fdddb44eed967bb2d4f60487665	https://github.com/TiKi-r/CVE-Report/blob/main/WtcmsRCE.md CISA-ADP, VulDB https://github.com/TiKi-r/CVE-Report/blob/main/WtcmsRCE.md#3-proof-of-concept-poc CISA-ADP, VulDB https://vuldb.com/?ctiid.333790 VulDB https://vuldb.com/?id.333790 VulDB https://vuldb.com/?submit.689523
https://nvd.nist.gov/vuln/detail/CVE-2025-58482	7,3	MPLocalService of MotionPhoto	Improper access control	prior to version 4.1.51	https://security.samsungmobile.com/serviceWeb.smsb?year=2025&month=12

https://nvd.nist.gov/vuln/detail/CVE-2025-13814	**7,3**	moxi159753 Mogu Blog	Server-Side Request Forgery (SSRF)	v2 up to 5.2	https://github.com/Xzzz111/exps/blob/main/archives/mogu_blog_v2-ssrf-1/report.md VulDB https://github.com/Xzzz111/exps/blob/main/archives/mogu_blog_v2-ssrf-1/report.md#proof-of-concept VulDB https://vuldb.com/?ctiid.333823 VulDB https://vuldb.com/?id.333823 VulDB https://vuldb.com/?submit.692105
https://nvd.nist.gov/vuln/detail/CVE-2025-13387	**7,2**	The Kadence WooCommerce Email Designer plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 1.5.17	https://plugins.trac.wordpress.org/changeset/3399955/kadence-woocommerce-email-designer Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/1e0cf512-f676-4f47-abaa-5198998376b7?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-66423	**7,1**	Tryton trytond	Incorrect Authorization	6.0 before 7.6.11	https://discuss.tryton.org/t/security-release-for-issue-14364/8952 MITRE https://foss.heptapod.net/tryton/tryton/-/issues/14364
https://nvd.nist.gov/vuln/detail/CVE-2025-66448	**7,1**	vLLM	Improper Control of Generation of Code ('Code Injection')	Prior to 0.11.1	https://github.com/vllm-project/vllm/commit/ffb08379d8870a1a81ba82b72797f196838d0c86 GitHub, Inc. https://github.com/vllm-project/vllm/pull/28126 GitHub, Inc. https://github.com/vllm-project/vllm/security/advisories/GHSA-8fr4-5q9j-m8gm
https://nvd.nist.gov/vuln/detail/CVE-2025-63365	**7,1**	SoftSea EPUB File Reader	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	1.0.0.0	http://epub.com MITRE https://jeroscope.com/advisories/2025/jero-2025-001/

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 One Known Exploited Vulnerability to Catalog	▪ **CVE-2021-26829 OpenPLC ScadaBR Cross-site Scripting Vulnerability**	**https://www.cisa.gov/news-events/alerts/2025/11/28/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
Tomiris Unleashes 'Havoc' With New Tools, Tactics	https://www.darkreading.com/cyberattacks-data-breaches/tomiris-unleashes-havoc-new-tools-tactics
Police Disrupt 'Cryptomixer,' Seize Millions in Crypto	https://www.darkreading.com/cyberattacks-data-breaches/police-disrupt-cryptomixer-seize-millions-crypto
Europol Takes Down Illegal Cryptocurrency Mixing Service	https://www.infosecurity-magazine.com/news/europol-takes-down-illegal/
India Mandates ‘Undeletable’ Government Cybersecurity App for All Smartphones	https://cybersecuritynews.com/india-mandates-cybersecurity-app/

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
South Korea’s Coupang Hit by Massive Data Breach Affecting Nearly 34 Million Customers	https://thecyberexpress.com/coupang-data-breach/?&web_view=true
Brit telco Brsk confirms breach as bidding begins for 230K+ customer records	https://www.theregister.com/2025/11/28/brsk_breach/?&web_view=true

Public GitLab repositories exposed more than 17,000 secrets	https://www.bleepingcomputer.com/news/security/public-gitlab-repositories-exposed-more-than-17-000-secrets/?&web_view=true
Canadian scientific consulting service confirms data breach following $1.2 million ransom demand	https://www.comparitech.com/news/canadian-scientific-consulting-service-confirms-data-breach-following-1-2-million-ransom-demand/?&web_view=true
Coupang Data Breach Exposed Personal Data of 33.7 Million Customers Personal Records	https://cybersecuritynews.com/coupang-data-breach/
4.3 Million Chrome and Edge Users Hacked in 7-Year ShadyPanda Malware Campaign	https://cybersecuritynews.com/4-3-million-chrome-and-edge-users-hacked/
Hackers Allegedly Claim Breach of Mercedes-Benz USA Legal and Customer Data	https://cybersecuritynews.com/mercedes-benz-breach-claim/
Hackers Registered 18,000 Holiday-Themed Domains Targeting 'Christmas,' 'Black Friday,' and 'Flash Sale'	https://cybersecuritynews.com/hackers-registered-18000-holiday-themed-domains/

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 Adds Actively Exploited XSS Bug CVE-2021-26829 in OpenPLC ScadaBR to KEV	https://thehackernews.com/2025/11/cisa-adds-actively-exploited-xss-bug.html
OpenVPN Vulnerabilities Let Hackers Triggers Dos Attack and Bypass Security Checks	https://cybersecuritynews.com/openvpn-vulnerabilities/
KimJongRAT Attacking Windows Users via Weaponized .hta Files to Steal Logins	https://cybersecuritynews.com/kimjongrat-attacking-windows-users/
Microsoft Confirms New Outlook Bug Blocking Excel Attachments	https://cybersecuritynews.com/microsoft-new-outlook-bug/
OpenAI Codex CLI Command Injection Vulnerability Let Attackers Execute Arbitrary Commands	https://cybersecuritynews.com/openai-codex-cli-vulnerability/
Microsoft Azure API Management Flaw Enables Cross-Tenant Account Creation, Bypassing Admin Restrictions	https://cybersecuritynews.com/microsoft-azure-api-management-flaw/
Critical Apache bRPC Framework Vulnerability Let Attackers Crash the Server	https://cybersecuritynews.com/apache-brpc-framework-vulnerability/
Windows 11 24H2 Update Hides the Password Icon in the Sign-in Options on the Lock Screen	https://cybersecuritynews.com/windows-11-24h2-update-hides-login/
PoC Exploit Released for Critical Outlook 0-Click Remote Code Execution Vulnerability	https://cybersecuritynews.com/outlook-remote-code-execution-vulnerability-2/
CISA Warns of OpenPLC ScadaBR cross-site scripting vulnerability Exploited in Attacks	https://cybersecuritynews.com/cisa-openplc-scadabr-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
Google Patches 107 Android Flaws, Including Two Framework Bugs Exploited in the Wild	https://thehackernews.com/2025/12/google-patches-107-android-flaws.html
Linux 6.18 Released With Enhanced Hardware Support, Updated Drivers and File Systems	https://cybersecuritynews.com/linux-6-18-released/

Potential threats / Threat intelligence

Η συγκεκριμένη ενότητα ασχολείται με νέες απειλές, εξελιγμένα malware και τεχνικές επιθέσεων που έχουν εντοπιστεί σε πραγματικές συν-θήκες. Περιλαμβάνονται αναφορές σε εργαλεία που χρησιμοποιούν οι επιτιθέμενοι, αλλά και δείκτες (IoCs) που μπορούν να χρησιμοποιηθούν στην άμυνα.

Σύντομη περιγραφή / Τίτλος	URL
Legacy Python Bootstrap Scripts Create Domain-Takeover Risk in Multiple PyPI Packages	https://thehackernews.com/2025/11/legacy-python-bootstrap-scripts-create.html
New Android Albiriox Malware Gains Traction in Dark Web Markets	**https://www.infosecurity-magazine.com/news/android-maas-malware-albiriox-dark/**
Malware Manipulates AI Detection in Latest npm Package Breach	https://www.infosecurity-magazine.com/news/malware-ai-detection-npm-package/
Operation Hanoi Thief Attacking IT Professionals with Pseudo-Polyglot Payload to Hide Malware	https://cybersecuritynews.com/operation-hanoi-thief-attacking-it-professionals/
Hackers Registered 2,000+ Fake Holiday-Themed Online Stores to Steal User Payments	https://cybersecuritynews.com/hackers-registered-2000-fake-holiday-themed-online-stores/
TangleCrypt Windows Packer with Ransomware Payloads Evades EDR Using ABYSSWORKER Driver	https://cybersecuritynews.com/tanglecrypt-windows-packer-with-ransomware-payloads/
Beware of Weaponized Google Meet Page uses ClickFix Technique to Deliver Malicious Payload	https://cybersecuritynews.com/weaponized-google-meet-clickfix/

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/
15 Best Remote Monitoring Tools – 2025	https://cybersecuritynews.com/best-remote-monitoring-tools/
Top 10 Best Exposure Management Tools In 2026	https://cybersecuritynews.com/best-exposure-management-tools/

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/