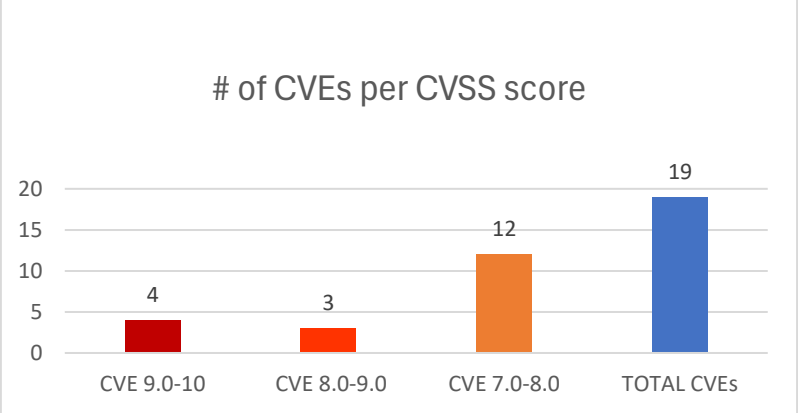
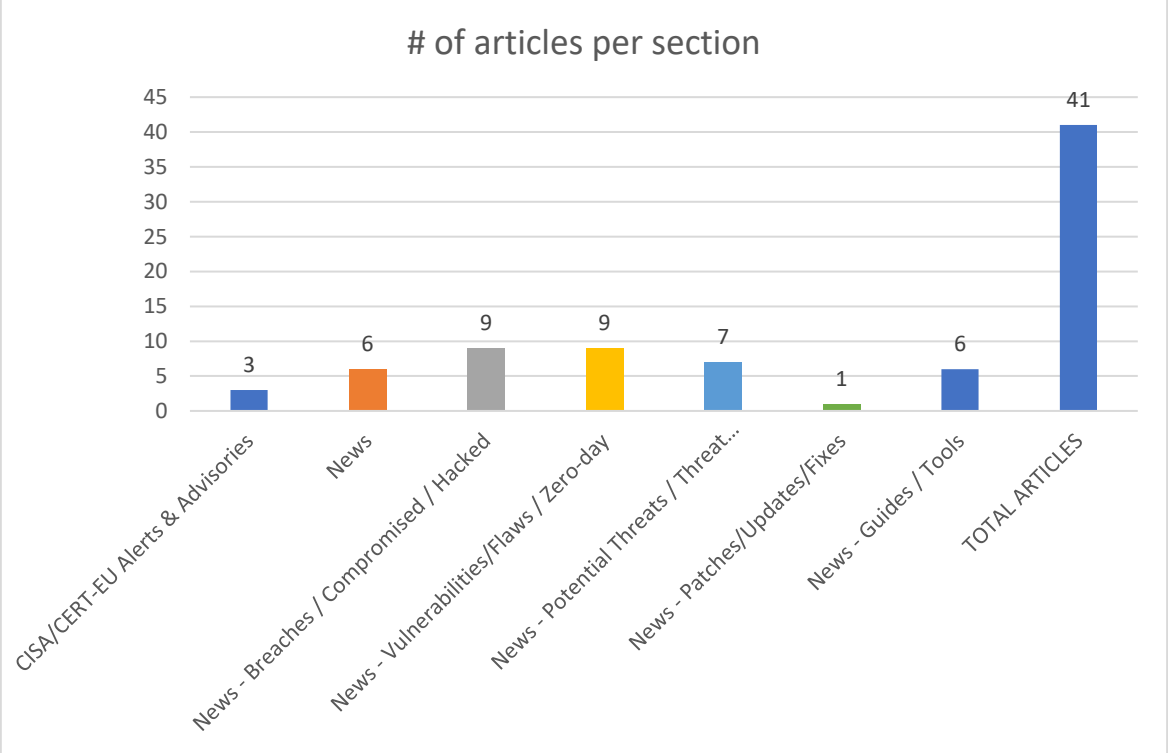
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 20/12/2025 - 23/12/2025





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-2025-15016	9,8	Enterprise Cloud Database developed by Ragic	Use of Hard-coded Cryptographic Key		https://www.twcert.org.tw/en/cp-139-10588-771e5-2.html TWCERT/CC https://www.twcert.org.tw/tw/cp-132-10587-797c6-1.html
https://nvd.nist.gov/vuln/detail/CVE-2025-15010	9,8	Tenda WH450	Stack-based Buffer Overflow	1.0.0.18	https://github.com/z472421519/BinaryAudit/blob/main/PoC/BOF/Tenda_WH450/SafeUrlFilter/SafeUrlFilter.md VulDB https://github.com/z472421519/BinaryAudit/blob/main/PoC/BOF/Tenda_WH450/SafeUrlFilter/SafeUrlFilter.md#reproduce VulDB https://vuldb.com/?ctiid.337716 VulDB https://vuldb.com/?id.337716 VulDB https://vuldb.com/?submit.719219 VulDB https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-13619	9,8	The Flex Store Users plugin for WordPress	Improper Privilege Management	up to, and including, 1.1.0	https://themeforest.net/item/autosmart-automotive-car-dealer-wordpress-theme/20322930 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/a2fc40ed-a6af-4069-be63-cb75e98cc98a?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-68669	9,6	5ire	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	0.15.2 and prior	https://github.com/nanbingxyz/5ire/blob/c40d05a2b546094789fc727daa5383bb15034442/src/hooks/useMarkdown.ts#L156 GitHub, Inc. https://github.com/nanbingxyz/5ire/releases/tag/v0.15.2 GitHub, Inc.

					https://github.com/nanbingxyz/5ire/security/advisories/GHSA-5hpf-p8fw-j349
https://nvd.nist.gov/vuln/detail/CVE-2025-14994	8,8	Tenda	Stack-based Buffer Overflow	FH1201 and FH1206 1.2.0.14(408)/ 1.2.0.8(8155)	https://github.com/z472421519/BinaryAudit/blob/main/PoC/BOF/Tenda_FH1201/webtypelibrary/webtypelibrary.md VulDB https://github.com/z472421519/BinaryAudit/blob/main/PoC/BOF/Tenda_FH1206/webtypelibrary/webtypelibrary.md VulDB https://vuldb.com/?ctiid.337688 VulDB https://vuldb.com/?id.337688 VulDB https://vuldb.com/?submit.719153 VulDB https://vuldb.com/?submit.719155 VulDB https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-68665	8,6	LangChain	Deserialization of Untrusted Data	0.3.80 and 1.1.8, and prior to langchain versions 0.3.37 and 1.2.3	https://github.com/langchain-ai/langchainjs/commit/e5063f9c6e9989ea067dfdff39262b9e7b6aba62 GitHub, Inc. https://github.com/langchain-ai/langchainjs/releases/tag/%40langchain%2Fcore%401.1.8 GitHub, Inc. https://github.com/langchain-ai/langchainjs/releases/tag/langchain%401.2.3 GitHub, Inc. https://github.com/langchain-ai/langchainjs/security/advisories/GHSA-r399-636x-v7f6
https://nvd.nist.gov/vuln/detail/CVE-2025-14800	8,1	The Redirection for Contact Form 7 plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 3.2.7	https://plugins.trac.wordpress.org/browser/wpcf7-redirect/tags/3.2.7/classes/class-wpcf7r-save-files.php#L180 Wordfence https://plugins.trac.wordpress.org/changeset/3423970/wpcf7-redirect Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/b249ec90-a364-4644-94fb-d42eb6cc4d9a?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-7782	7,6	The WP JobHunt plugin for WordPress	Missing Authorization	up to, and including, 7.7	https://themeforest.net/item/jobcareer-job-board-responsive-wordpress-theme/14221636 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/af063570-43f7-4bf4-850c-21c3bff40ac1?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-68561	7,6	Ruben Garcia AutomatorWP	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	from n/a through 5.2.4	https://vdp.patchstack.com/database/wordpress/plugin/automatorwp/vulnerability/wordpress-automatorwp-plugin-5-2-4-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-14071	7,5	The Live Composer – Free WordPress Website Builder plugin for WordPress	Deserialization of Untrusted Data	up to, and including, 2.0.2	https://github.com/live-composer/live-composer-page-builder/commit/2b0b430ab107eb6cb72196251e429a695c11e41b Wordfence https://plugins.trac.wordpress.org/browser/live-composer-page-builder/tags/1.5.53/modules/posts/module.php#L2807 Wordfence https://plugins.trac.wordpress.org/browser/live-composer-page-builder/trunk/modules/posts/module.php#L2807 Wordfence https://plugins.trac.wordpress.org/changeset/3419715/live-composer-page-builder/trunk/modules/posts/module.php Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/4b15c991-5256-405c-8382-85dba6f032ba?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-12980	7,5	The Post Grid Gutenberg Blocks for News, Magazines, Blog Websites – PostX plugin for WordPress	Missing Authorization	up to, and including, 5.0.3	https://plugins.trac.wordpress.org/changeset/3421729/ultimate-post/trunk/classes/Blocks.php Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/e85ff3b3-de41-4ac4-b825-b3238725ca44?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-68546	7,5	Thembay Nika	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion	from n/a through 1.2.14	https://vdp.patchstack.com/database/wordpress/theme/nika/vulnerability/wordpress-nika-theme-1-2-14-local-file-inclusion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-68644	7,4	Yealink RPS	Authentication Bypass by Spoofing	before 2025-06-27	https://www.yealink.com/en/trust-center/security-bulletins/yealink-unauthorized-access-to-rps-vulnerability MITRE https://www.yealink.com/website-service/download/Yealink_RPS_Security_Remediation_Verification_Report.pdf
https://nvd.nist.gov/vuln/detail/CVE-2025-15012	7,3	Refugee Food Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ VulDB https://github.com/jjjjj-zr/jjjjjzr17/issues/2 VulDB https://vuldb.com/?ctiid.337718 VulDB https://vuldb.com/?id.337718 VulDB https://vuldb.com/?submit.719788
https://nvd.nist.gov/vuln/detail/CVE-2025-15011	7,3	Simple Stock System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ VulDB https://github.com/chunmingshanan/CVE/issues/1 VulDB https://vuldb.com/?ctiid.337717 VulDB https://vuldb.com/?id.337717 VulDB https://vuldb.com/?submit.719663
https://nvd.nist.gov/vuln/detail/CVE-2025-15002	7,3	SeaCMS	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to 13.3	https://note-hxlab.wetolink.com/share/VFwALb6qhnTZ VulDB https://vuldb.com/?ctiid.337707 VulDB https://vuldb.com/?id.337707 VulDB https://vuldb.com/?submit.716083

https://nvd.nist.gov/vuln/detail/CVE-2025-14990	7,3	Campcodes Complete Online Beauty Parlor Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/funnnxxx/my-cve/issues/2 VulDB https://vuldb.com/?ctiid.337684 VulDB https://vuldb.com/?id.337684 VulDB https://vuldb.com/?submit.718453 VulDB https://www.campcodes.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-9343	7,2	The ELEX WordPress HelpDesk & Customer Ticketing System plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	all versions up to, and including, 3.3.4	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3420695%40elex-helpdesk-customer-support-ticket-system&new=3420695%40elex-helpdesk-customer-support-ticket-system&sfp_email=&sfph_mail= Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/042d9bc7-50ea-4585-9789-b10ed40b0d14?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-14855	7,2	The SureForms plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 2.2.0	https://plugins.trac.wordpress.org/browser/sureforms/tags/2.2.0/assets/build/entries.js Wordfence https://plugins.trac.wordpress.org/changeset/3423684/sureforms Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/5e493f01-95db-48ba-8daf-d7ff69df29bf?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 Releases One Industrial Control Systems Advisory	▪ **ICSA-25-177-01 Mitsubishi Electric Air Conditioning Systems (Update B)**	**https://www.cisa.gov/news-events/alerts/2025/12/23/cisa-releases-one-industrial-control-systems-advisory**
CISA Adds One Known Exploited Vulnerability to Catalog	▪ **CVE-2023-52163 Digiever DS-2105 Pro Missing Authorization Vulnerability**	**https://www.cisa.gov/news-events/alerts/2025/12/22/cisa-adds-one-known-exploited-vulnerability-catalog**
NIST and CISA Release Draft Interagency Report on Protecting Tokens and Assertions from Tampering Theft and Misuse for Public Comment	▪	**https://www.cisa.gov/news-events/alerts/2025/12/22/nist-and-cisa-release-draft-interagency-report-protecting-tokens-and-assertions-tampering-theft-and**

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
Claude Opus 4.5 Now Integrated with GitHub Copilot	**https://cybersecuritynews.com/claude-opus-4-5-integrated-with-github-copilot/**
CISA Releases New Indicators of Compromise Tied to BRICKSTORM Malware	**https://cybersecuritynews.com/cisa-releases-indicators-of-compromise-tied-to-brickstorm-malware/**
Scripted Sparrow Sends Millions of BEC Emails Each Month	**https://www.infosecurity-magazine.com/news/scripted-sparrow-millions-bec-each/**
UK: NHS Supplier Confirms Cyber-Attack, Operations Unaffected	**https://www.infosecurity-magazine.com/news/uk-nhs-supplier-confirms/**
Amazon Fends Off 1,800 Suspected DPRK IT Job Scammers	**https://www.darkreading.com/remote-workforce/amazon-fends-off-dprk-it-job-scammers**
Nefilim Ransomware Affiliate Pleads Guilty	**https://www.infosecurity-magazine.com/news/nefilim-ransomware-affiliate/**

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
Cybersecurity Weekly Recap – PornHub Breach, Cisco 0-Day, Amazon Detains DPRK IT Worker, and more	**https://cybersecuritynews.com/cybersecurity-newsletter-december/**
100+ Cisco Secure Email Devices Exposed to Zero-Day Exploited in the Wild	**https://cybersecuritynews.com/cisco-secure-email-devices-zero-day/**
125,000 IPs WatchGuard Firebox Devices Exposed to Internet Vulnerable to 0-day RCE Attacks	**https://cybersecuritynews.com/125000-ips-watchguard-firebox-devices/**
Around 1,000 systems compromised in ransomware attack on Romanian water agency	https://www.theregister.com/2025/12/22/around_1000_systems_compromised_in/?&web_view=true
University of Phoenix data breach impacts nearly 3.5 million individuals	https://www.bleepingcomputer.com/news/security/university-of-phoenix-data-breach-impacts-nearly-35-million-individuals/?&web_view=true
Florida dermatologist warns 55,000+ people of data breach that compromised SSNs, medical info	https://www.comparitech.com/news/florida-dermatologist-warns-55000-people-of-data-breach-that-compromised-ssns-medical-info/?&web_view=true
Nissan: Thousands Impacted By Red Hat Breach	https://www.infosecurity-magazine.com/news/nissan-thousands-impacted-by-red/
Spotify Music Library With 86M Music Files Scraped by Hacktivist Group	https://cybersecuritynews.com/spotify-music-library-scraped/
Malicious NPM Package with 56K Downloads Steals WhatsApp Messages	https://cybersecuritynews.com/malicious-npm-package-with-56k-downloads/

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
Critical RCE flaw impacts over 115,000 WatchGuard firewalls	**https://www.bleepingcomputer.com/news/security/over-115-000-watchguard-firewalls-vulnerable-to-ongoing-rce-attacks/**

Multiple Exim Server Vulnerabilities Let Attackers Seize Control of the Server	**https://cybersecuritynews.com/exim-server-vulnerabilities/**
Critical n8n Flaw (CVSS 9.9) Enables Arbitrary Code Execution Across Thousands of Instances	**https://thehackernews.com/2025/12/critical-n8n-flaw-cvss-99-enables.html**
Windows Imaging Component Vulnerability Can Lead to RCE Attacks Under Complex Attack Scenarios	**https://cybersecuritynews.com/windows-imaging-component-vulnerability/**
PoC Exploit Released HPE OneView Vulnerability that Enables Remote Code Execution	**https://cybersecuritynews.com/poc-exploit-hpe-oneview-vulnerability/**
CISA Adds Digiever Authorization Vulnerability to KEV List Following Active Exploitation	**https://cybersecuritynews.com/cisa-adds-digiever-authorization-vulnerability/**
Hackers Using ClickFix Technique to Hide Images within the Image Files	**https://cybersecuritynews.com/hackers-using-clickfix-technique/**
PoC Exploit Released for Use-After-Free Vulnerability in Linux Kernel's POSIX CPU Timers Implementation	**https://cybersecuritynews.com/use-after-free-vulnerability-linux-kernel/**
Sleeping Bouncer Vulnerability Impacts Motherboards from Gigabyte, MSI, ASRock and ASUS	**https://cybersecuritynews.com/sleeping-bouncer-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
WatchGuard Patches Firebox Zero-Day Exploited in the Wild	**https://www.securityweek.com/watchguard-patches-firebox-zero-day-exploited-in-the-wild/**

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 Weaponize SVG Files and Office Documents to Target Windows Users	**https://cybersecuritynews.com/hackers-weaponize-svg-files-and-office-documents/**
Hackers Using Phishing Tools to Access M365 Accounts via OAuth Device Code	**https://cybersecuritynews.com/hackers-using-phishing-tools/**
DIG AI – Darknet AI Tool Enabling Threat Actors to Launch Sophisticated Attacks	**https://cybersecuritynews.com/dig-ai-darknet-ai-tool/**

Uzbek Users Under Attack by Android SMS-Stealers	https://www.darkreading.com/cyber-risk/uzbek-users-android-sms-stealers
HardBit 4.0 Ransomware Actors Attack Open RDP and SMB Services to Persist Access	https://cybersecuritynews.com/hardbit-4-0-ransomware-actors-attack-open-rdp/
New MacSync Stealer Malware Attacking macOS Users Using Digitally Signed Apps	https://cybersecuritynews.com/new-macsync-stealer-malware/
Threat Actors Weaponizing Nezha Monitoring Tool as Remote Access Trojan	https://cybersecuritynews.com/threat-actors-weaponizing-nezha-monitoring-tool/

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/