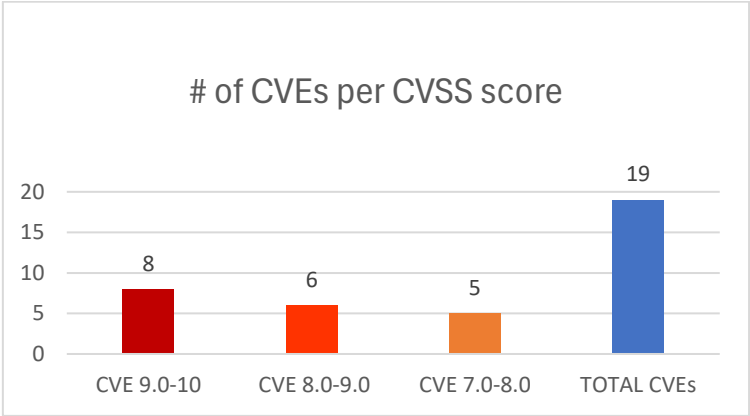
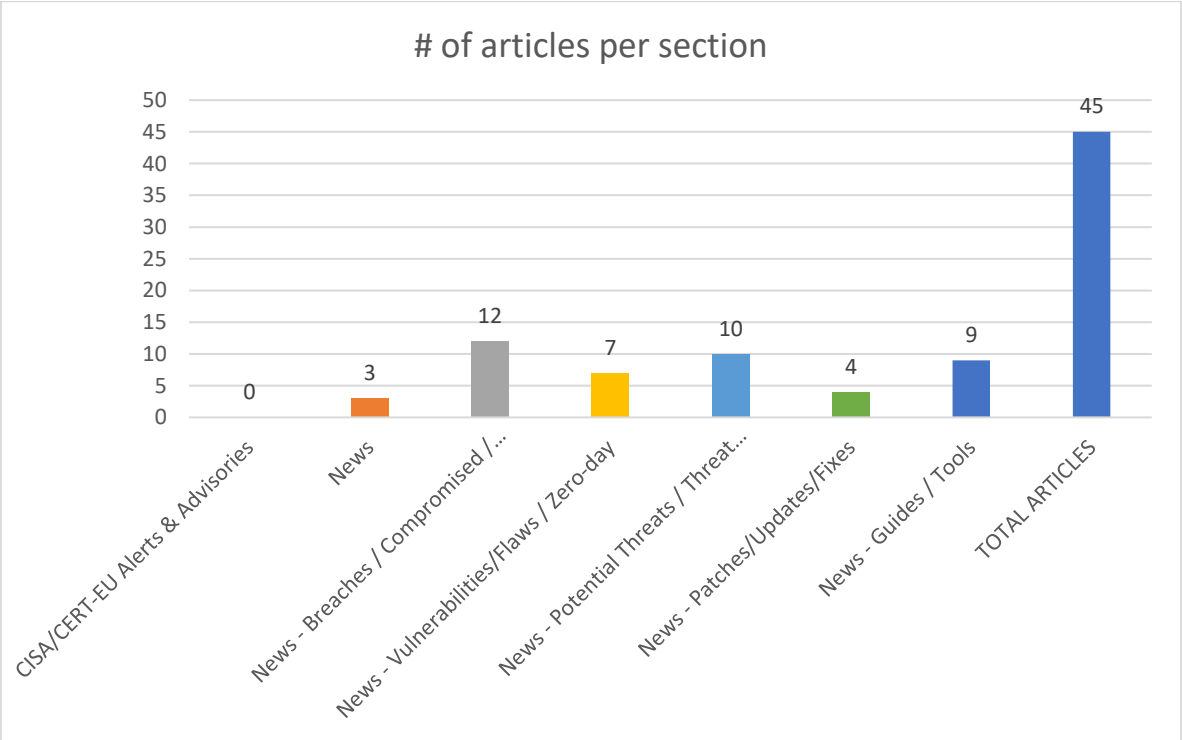
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 26/11/2025 - 28/11/2025





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-2025-13595	9,8	The CIBELES AI plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 1.10.8	https://github.com/d0n601/CVE-2025-13595 Wordfence https://plugins.trac.wordpress.org/browser/cibeles-ai/trunk/actualizador_git.php#L1 Wordfence https://plugins.trac.wordpress.org/changeset/3402311/cibeles-ai Wordfence https://ryankozak.com/posts/cve-2025-13595/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/b3e89a1c-7606-4391-a389-fa18d0967046?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-13597	9,8	The AI Feeds plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 1.0.11.	https://github.com/d0n601/CVE-2025-13597 Wordfence https://plugins.trac.wordpress.org/browser/ai-feeds/trunk/actualizador_git.php#L1 Wordfence https://plugins.trac.wordpress.org/changeset/3402321/ai-feeds Wordfence https://ryankozak.com/posts/cve-2025-13597 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/c5007dd0-a62c-4ad8-8f8b-eb3f4387c370?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-64657	9,8	Azure Application Gateway	Stack-based Buffer Overflow		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-64657
https://nvd.nist.gov/vuln/detail/CVE-2025-64130	9,8	Zenitel TCIV-3+	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')		https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2025/icsa-25-329-03.json ICS-CERT https://wiki.zenitel.com/wiki/Downloads#Station_and_Device_Firmware_Package_.28VS-IS.29 ICS-CERT https://www.cisa.gov/news-events/ics-advisories/icsa-25-329-03
https://nvd.nist.gov/vuln/detail/CVE-2025-59390	9,8	Apache Druid's Kerberos	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	through 34.0.0	http://www.openwall.com/lists/oss-security/2025/11/26/1 CVE https://lists.apache.org/thread/jwjltllnntgj1sb9wzsjmvwm9f8rlhg8
https://nvd.nist.gov/vuln/detail/CVE-2025-62354	9,8	OS command ('command injection') in Cursor	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')		https://hiddenlayer.com/sai_security_advisor/2025-11-cursor/

https://nvd.nist.gov/vuln/detail/CVE-2025-13540	9,8	The Tiare Membership plugin for WordPress	Improper Privilege Management	up to, and including, 1.2	https://themeforest.net/item/tiare-wedding-vendor-directory-theme/26589165?s_rank=1 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/6cf01a38-1fba-4c93-b3fa-acfdd5b19410?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-13538	9,8	The FindAll Listing plugin for WordPress	Improper Privilege Management	up to, and including, 1.0.5	https://themeforest.net/item/findall-business-directory-theme/24415962 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/14981949-271c-4f98-a6a1-b00619f1436d?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-13680	8,8	The Tiger theme for WordPress	Improper Privilege Management	up to, and including, 101.2.1	https://themeforest.net/item/tiger-social-network-theme-for-companies-professionals/16203995 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/645f60ad-c8e5-47ec-94f1-960de4ef7838?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-13536	8,8	The Blubrry PowerPress plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 11.15.2	https://plugins.trac.wordpress.org/browser/powerpress/tags/11.14.1/powerpressadmin.php#L2368 Wordfence https://plugins.trac.wordpress.org/browser/powerpress/tags/11.14.1/powerpressadmin.php#L3012 Wordfence https://plugins.trac.wordpress.org/browser/powerpress/tags/11.14.1/powerpressadmin.php#L3068 Wordfence https://plugins.trac.wordpress.org/changeset/3402635/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/d420ee49-e7b3-43d8-a263-8a93abd1133c?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-12816	8,6	node-forge	Interpretation Conflict	1.3.1 and earlier	https://github.com/digitalbazaar/forge CERT/CC https://github.com/digitalbazaar/forge/pull/1124 CERT/CC https://github.com/digitalbazaar/forge/security/advisories/GHSA-5gfm-wpxj-wjgq CERT/CC https://kb.cert.org/vuls/id/521113 CERT/CC https://www.kb.cert.org/vuls/id/521113 CVE https://www.npmjs.com/package/node-forge
https://nvd.nist.gov/vuln/detail/CVE-2025-66359	8,5	Logpoint	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	before 7.7.0	https://servicedesk.logpoint.com/hc/en-us/articles/29158899698333-XSS-Vulnerability-due-to-insufficient-input-validation
https://nvd.nist.gov/vuln/detail/CVE-2025-66384	8,2	app/Controller/EventsController.php in MISP	Incorrect Provision of Specified Functionality	before 2.5.24	https://github.com/MISP/MISP/compare/v2.5.23...v2.5.24 MITRE https://github.com/misp/misp/commit/6867f0d3157a1959154bdad9ddac009dec6a19f5
https://nvd.nist.gov/vuln/detail/CVE-2025-64983	8,0	Smart Video Doorbell firmware	Active Debug Code	prior to 2.01.078	https://jvn.jp/en/jp/JVN67185535 JPCERT/CC https://www.switch-bot.com/products/switchbot-video-doorbell?srsltid=AfmBOooGEZArqUag9p59qB8ti2fDP0vCOzxX33NGlpJ8yDlZ-nzC3vJ_f

https://nvd.nist.gov/vuln/detail/CVE-2025-66020	7,5	Valibot	Inefficient Regular Expression Complexity	from 0.31.0 to 1.1.0	https://github.com/open-circle/valibot/commit/cfb799db301a953a0950d5c05a34a3ab121262dc GitHub, Inc. https://github.com/open-circle/valibot/security/advisories/GHSA-vqpr-j7v3-hqw9
https://nvd.nist.gov/vuln/detail/CVE-2025-7820	7,5	The SKT PayPal for WooCommerce plugin for WordPress	Client-Side Enforcement of Server-Side Security	up to, and including, 1.4	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3403118%40skt-paypal-for-woocommerce&new=3403118%40skt-paypal-for-woocommerce&sfp_email=&sfph_mail= Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/1a67b1b3-eb39-4e9a-ba44-ea637fc3bba1?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-66314	7,5	ZTE ElasticNet UME R32	Improper Privilege Management	ElasticNet_UME_R32_V16.23.20.04	https://support.zte.com.cn/zte-iccp-isupport-webui/bulletin/detail/2180460616364429350
https://nvd.nist.gov/vuln/detail/CVE-2025-64344	7,5	Suricata	Stack-based Buffer Overflow	Prior to versions 7.0.13 and 8.0.2	https://github.com/OISF/suricata/commit/e13fe6a90dba210a478148c4084f6f5db17c5b5a GitHub, Inc. https://github.com/OISF/suricata/security/advisories/GHSA-93fh-cgmc-w3rx
https://nvd.nist.gov/vuln/detail/CVE-2025-13692	7,2	The Unlimited Elements For Elementor plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 2.0	https://plugins.trac.wordpress.org/browser/unlimited-elements-for-elementor/trunk/inc_php/unitecreator_filters_process.class.php#L3279 Wordfence https://plugins.trac.wordpress.org/browser/unlimited-elements-for-elementor/trunk/inc_php/unitecreator_form.class.php#L1952 Wordfence https://plugins.trac.wordpress.org/browser/unlimited-elements-for-elementor/trunk/inc_php/unitecreator_form.class.php#L1960 Wordfence https://plugins.trac.wordpress.org/browser/unlimited-elements-for-elementor/trunk/inc_php/unitecreator_form.class.php#L598 Wordfence https://plugins.trac.wordpress.org/changeset/3403331/ Wordfence https://unlimited-elements.com/change-log/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/ae603b13-dc09-4f83-8741-943d62615b3c?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

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
FBI Reports $262M in ATO Fraud as Researchers Cite Growing AI Phishing and Holiday Scams	https://thehackernews.com/2025/11/fbi-reports-262m-in-ato-fraud-as.html
FCC Warns of Hackers Hijacking Radio Equipment For False Alerts	https://www.infosecurity-magazine.com/news/fcc-hackers-hijacking-radio/
Microsoft Security Keys May Require PIN After Recent Windows Updates	https://cybersecuritynews.com/microsoft-security-keys-may-require-pin/

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
Multiple London councils report disruption amid ongoing cyberattack	https://techcrunch.com/2025/11/26/multiple-london-councils-report-disruption-amid-ongoing-cyberattack/?&web_view=true
Qilin Ransomware Turns South Korean MSP Breach Into 28-Victim 'Korean Leaks' Data Heist	https://thehackernews.com/2025/11/qilin-ransomware-turns-south-korean-msp.html?&web_view=true
OpenAI Confirms Mixpanel Breach Impacting API User Data	https://thecyberexpress.com/openai-mixpanel-security-incident/?&web_view=true

London Councils Hit By Serious Cyber "Incidents"	https://www.infosecurity-magazine.com/news/london-councils-hit-by-serious/?&web_view=true
OnSolve CodeRED cyberattack disrupts emergency alert systems nationwide	https://www.bleepingcomputer.com/news/security/onsolve-codered-cyberattack-disrupts-emergency-alert-systems-nationwide/?&web_view=true
Asahi Confirms 1.5 Million Customers Affected in Major Cyber-Attack	https://www.infosecurity-magazine.com/news/asahi-15-million-customers/
Cyber-Attack Disrupts OnSolve CodeRED Emergency Notification System	https://www.infosecurity-magazine.com/news/cyberattack-disrupts-onsolve/
Shai Hulud 2.0 Compromises 1,200+ Organizations, Exposing Critical Runtime Secrets	https://cybersecuritynews.com/shai-hulud-2-0/
Scattered Lapsus$ Hunters Registered 40+ Domains Mimicking Zendesk Environments	https://cybersecuritynews.com/scattered-lapsus-hunters-registered-40-domains/
Dead Man's Switch – Widespread npm Supply Chain Attack Driving Malware Attacks	https://cybersecuritynews.com/dead-mans-switch-npm-supply-chain-attack/
OpenAI Discloses Mixpanel Data Breach – Name, Email Address and Operating System Details Exposed	https://cybersecuritynews.com/openai-discloses-mixpanel-data-breach/
Developers Expose Passwords and API Keys via Online Tools like JSONFormatter	https://cybersecuritynews.com/developers-expose-passwords-and-api-keys/

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
Fluent Bit Vulnerabilities Expose Cloud Services to Takeover	https://www.securityweek.com/fluent-bit-vulnerabilities-expose-cloud-services-to-takeover/
NVIDIA DGX Spark Vulnerabilities Let Attackers Execute Malicious Code and DoS Attacks	https://cybersecuritynews.com/nvidia-dgx-spark-vulnerabilities/
Hackers Actively Exploiting IoT Vulnerabilities to Deploy New ShadowV2 Malware	https://cybersecuritynews.com/hackers-exploiting-iot-flaws-to-deployshadowv2/
Angular HTTP Client Vulnerability Exposes XSRF Token to an Attacker-Controlled Domain	https://cybersecuritynews.com/angular-http-client-vulnerability/
Threat Actors Allegedly Listed iOS 26 Full-Chain 0-Day Exploit on Dark Web	https://cybersecuritynews.com/ios-26-full%e2%80%91chain-0%e2%80%91day-exploit/
Apache Syncope Vulnerability Allows Attacker to Access Internal Database Content	https://cybersecuritynews.com/apache-syncope-vulnerability/
Indirect-Shellcode-Executor Tool Exploits Windows API Vulnerability to Evade AV and EDR	https://cybersecuritynews.com/indirect-shellcode-executor-evade-av-and-edr/

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
Popular Forge library gets fix for signature verification bypass flaw	https://www.bleepingcomputer.com/news/security/popular-forge-library-gets-fix-for-signature-verification-bypass-flaw/
Gitlab Patches Multiple Vulnerabilities that Enable Authentication Bypass and DoS Attacks	https://cybersecuritynews.com/gitlab-patches-vulnerabilities/
Cobalt Strike 4.12 Released With New Process Injection, UAC Bypasses and Malleable C2 Options	https://cybersecuritynews.com/cobalt-strike-4-12-released/
Microsoft Teams Introduces New Feature to Boost Performance and Startup Speed	https://cybersecuritynews.com/microsoft-teams-introduces-new-feature-to-boost-performance/

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
New ShadowV2 botnet malware used AWS outage as a test opportunity	https://www.bleepingcomputer.com/news/security/new-shadowv2-botnet-malware-used-aws-outage-as-a-test-opportunity/
HashJack Indirect Prompt Injection Weaponizes Websites	**https://www.infosecurity-magazine.com/news/hashjack-indirect-prompt-injection/**
Scattered Lapsus$ Hunters Take Aim At Zendesk Users	https://www.infosecurity-magazine.com/news/scattered-lapsus-hunters-zendesk/
Vulnerable Codes in Legacy Python Packages Enables Attacks on Python Package Index Via Domain Compromise	https://cybersecuritynews.com/vulnerable-codes-in-legacy-python-packages/
Over 390 Abandoned iCalendar Sync Domains Could Expose ~4 Million Devices to Security Risks	https://cybersecuritynews.com/over-390-abandoned-icalendar-sync-domains-could-expose/
KawaiiGPT – Free WormGPT Variant Leveraging DeepSeek, Gemini, and Kimi-K2 AI Models	https://cybersecuritynews.com/kawaiigpt-free-wormgpt-variant/
Malicious Chrome Extension Silently Steal and Injects Hidden SOL Fees Into Solana Swaps	https://cybersecuritynews.com/malicious-chrome-extension/
Water Gamayun Hackers Exploit Windows MSC EvilTwin 0-Day to Inject Stealthy Malware	https://cybersecuritynews.com/water-gamayun-apt-hackers-exploit-msc/
Akira Ransomware Uses SonicWall VPN Exploit to Exfiltrate Sensitive Data	https://cybersecuritynews.com/akira-ransomware-uses-sonicwall-vpn-exploit/
New “JackFix” Attack Leverages Windows Updates into Executing Malicious Commands	https://cybersecuritynews.com/jackfix-attack-leverages-windows-updates/

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/