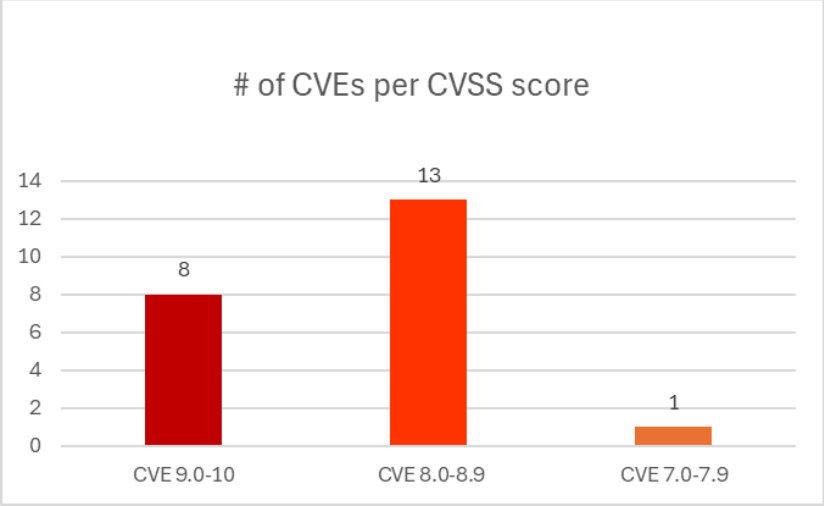
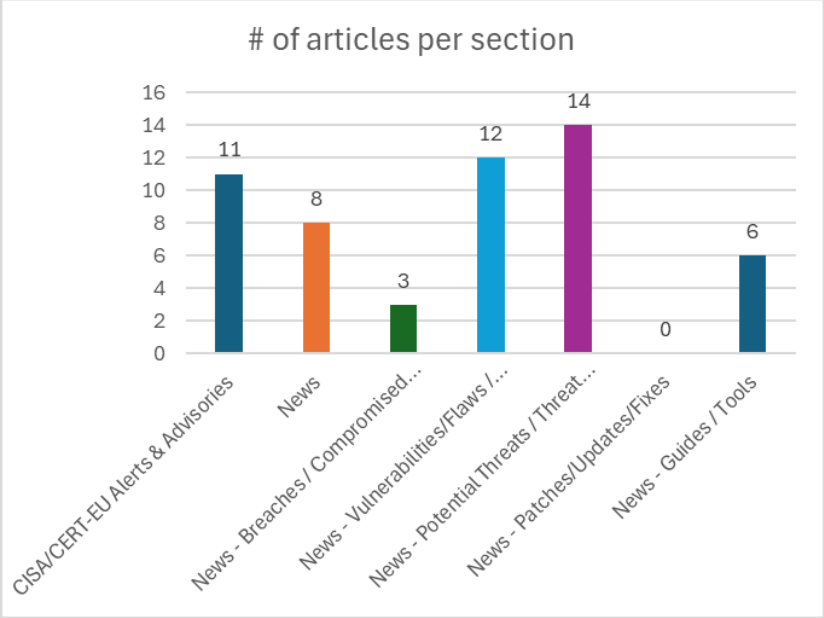
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 10/01/2026 - 13/01/2026





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)	CVSSv 3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2025-52694	10	Advantech	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')		https://www.csa.gov.sg/alerts-and-advisories/alerts/alerts-al-2026-001/
https://nvd.nist.gov/vuln/detail/CVE-2025-63314	10	DDSN Interactive Acora CMS	Weak Password Recovery Mechanism for Forgotten Password	DDSN Interactive Acora CMS v10.7.1	http://acora.com http://ddsn.com https://github.com/padayali-JD/CVE-2025-63314
https://nvd.nist.gov/vuln/detail/CVE-2026-22781	10	TinyWeb	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	before version 1.98	https://github.com/maximmasiutin/TinyWeb/commit/876b7e2887f4ea5be3e18bb2af7313f23a283c96 https://github.com/maximmasiutin/TinyWeb/security/advisories/GHSA-m779-84h5-72q2 https://www.masiutin.net/tinyweb-cve-2025-cgi-command-injection.html
https://nvd.nist.gov/vuln/detail/CVE-2026-22783	9,6	Iris	External Control of File Name or Path	Prior to 2.4.24	https://github.com/dfir-iris/iris-web/commit/57c1b80494bac187893aebc6d9df1ce6e56485b7 https://github.com/dfir-iris/iris-web/security/advisories/GHSA-qhqj-8qw6-wp8v

https://nvd.nist.gov/vuln/detail/CVE-2026-22794	9,6	Appsmith	Origin Validation Error	Prior to 1.93	https://github.com/appsmithorg/appsmith/commit/6f9ee6226bac13fb4b836940b557913fff78b633 https://github.com/appsmithorg/appsmith/security/advisories/GHSA-7hf5-mc28-xmcv
https://nvd.nist.gov/vuln/detail/CVE-2026-0491	9,1	SAP Landscape Transformation	Improper Control of Generation of Code ('Code Injection')		https://me.sap.com/notes/3697979 https://url.sap/sapsecuritypatchday
https://nvd.nist.gov/vuln/detail/CVE-2026-0498	9,1	SAP S/4HANA (Private Cloud and On-Premise)	Improper Control of Generation of Code ('Code Injection')		https://me.sap.com/notes/3694242 https://url.sap/sapsecuritypatchday
https://nvd.nist.gov/vuln/detail/CVE-2026-22252	9,1	LibreChat	Improper Authorization	Prior to v0.8.2-rc2	https://github.com/danny-avila/LibreChat/commit/211b39f3113d4e6ecab84be0a83f4e9c9dea127f https://github.com/danny-avila/LibreChat/security/advisories/GHSA-cxhj-j78r-p88f
https://nvd.nist.gov/vuln/detail/CVE-2025-66177	8,8	Hikvision		Hikvision NVR/DVR/CVR/IPC models	https://www.hikvision.com/en/support/cybersecurity/security-advisory/buffer-overflow-vulnerabilities-in-some-hikvision-products/
https://nvd.nist.gov/vuln/detail/CVE-2026-0841	8,8	UTT 进取 520W	Improper Restriction of Operations within the Bounds of a Memory Buffer	1.7.7-180627	https://github.com/GUOTINGTING2297/cve/blob/main/1234/31.md https://vuldb.com/?ctiid.340441 https://vuldb.com/?id.340441 https://vuldb.com/?submit.729030

https://nvd.nist.gov/vuln/detail/CVE-2026-0855	**8,8**	Merit LILIN	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Certain IP Camera models developed by Merit LILIN has a OS Command Injection vulnerability, allowing authenticated remote attackers to inject arbitrary OS commands and execute them on the device.	https://www.twcert.org.tw/en/cp-139-10626-afbe2-2.html https://www.twcert.org.tw/tw/cp-132-10625-fac5c-1.html
https://nvd.nist.gov/vuln/detail/CVE-2026-22685	**8,8**	DevToys	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	In versions from 2.0.0.0 to before 2.0.9.0	https://github.com/DevToys-app/DevToys/commit/02fb7d46d9c663a4ee6ed968baa6a8810405047f https://github.com/DevToys-app/DevToys/pull/1643 https://github.com/DevToys-app/DevToys/security/advisories/GHSA-ggxr-h6fm-p2qh
https://nvd.nist.gov/vuln/detail/CVE-2026-22771	**8,8**	Envoy Gateway	Improper Control of Generation of Code ('Code Injection')	Prior to 1.5.7 and 1.6.2	https://github.com/envoyproxy/gateway/security/advisories/GHSA-xrwg-mqj6-6m22
https://nvd.nist.gov/vuln/detail/CVE-2026-22812	**8,8**	OpenCod	Missing Authentication for Critical Function	Prior to 1.0.216	https://github.com/anomalyco/opencode/security/advisories/GHSA-vxw4-wv6m-9hhh
https://nvd.nist.gov/vuln/detail/CVE-2025-69273	**8,7**	Broadcom DX NetOps Spectrum	Improper Authentication	DX NetOps Spectrum: 24.3.10 and earlier	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36756

https://nvd.nist.gov/vuln/detail/CVE-2025-71063	**8,2**	Errands	Improper Certificate Validation		https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1123738 https://github.com/mrvladus/Errands/commit/04e567b432083fc798ea2249363ea6c83ff01099 https://github.com/mrvladus/Errands/compare/46.2.9...46.2.10 https://github.com/mrvladus/Errands/issues/401 https://github.com/mrvladus/Errands/releases/tag/46.2.10
https://nvd.nist.gov/vuln/detail/CVE-2026-22788	**8,2**	WebErpMesv2	Missing Authentication for Critical Function	Prior to 1.19	https://github.com/SMEWebify/WebErpMesv2/commit/3a7ab1c95d1d1c8f7c62c84bc87b3666ecd2fa23 https://github.com/SMEWebify/WebErpMesv2/security/advisories/GHSA-pp68-5pc2-hv7w
https://nvd.nist.gov/vuln/detail/CVE-2025-62235	**8,1**	Apache NimBLE	Authentication Bypass by Spoofing	This issue affects Apache NimBLE: through 1.8.0	http://www.openwall.com/lists/oss-security/2026/01/08/4 https://github.com/apache/mynewt-nimble/commit/41f67e391e788c5feef9030026cc5cbc5431838a https://lists.apache.org/thread/rw2mrpfwb9d9wmq4h4b6ctcd6gpkk2ho
https://nvd.nist.gov/vuln/detail/CVE-2025-68493	**8,1**	Apache Struts	Missing XML Validation	from 2.0.0 before 2.2.1	ttp://www.openwall.com/lists/oss-security/2026/01/11/2 https://cwiki.apache.org/confluence/display/WW/S2-069
https://nvd.nist.gov/vuln/detail/CVE-2026-0511	**8,1**	SAP Fiori App Intercompany Balance Reconciliation	Missing Authorization		https://me.sap.com/notes/3565506 https://url.sap/sapsecuritypatchday
https://nvd.nist.gov/vuln/detail/CVE-2026-22804	**8,0**	Termix	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	From 1.7.0 to 1.9.0	https://github.com/Termix-SSH/Termix/security/advisories/GHSA-m3cv-5hgp-hv35
https://nvd.nist.gov/vuln/detail/CVE-2026-22700	**7,5**	RustCrypto	Improper Input Validation	In versions 0.14.0-pre.0 and 0.14.0-rc.0	https://github.com/RustCrypto/elliptic-curves/commit/e60e99167a9a2b187ebe80c994c5204b0fdaf4ab https://github.com/RustCrypto/elliptic-curves/pull/1603 https://github.com/RustCrypto/elliptic-curves/security/advisories/GHSA-j9xq-69pf-pcm8

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-2025-8110 Gogs Path Traversal Vulnerability	https://www.cisa.gov/news-events/alerts/2026/01/12/cisa-adds-one-known-exploited-vulnerability-catalog
Vulnerability Summary for the Week of January 5, 2026		https://www.cisa.gov/news-events/bulletins/sb26-012
ED 24-02: Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System (Closed)		https://www.cisa.gov/news-events/directives/ed-24-02-mitigating-significant-risk-nation-state-compromise-microsoft-corporate-email-system-closed
ED 22-03: Mitigate VMware Vulnerabilities (Closed)		https://www.cisa.gov/news-events/directives/ed-22-03-mitigate-vmware-vulnerabilities-closed
ED 21-04: Mitigate Windows Print Spooler Service Vulnerability (Closed)		https://www.cisa.gov/news-events/directives/ed-21-04-mitigate-windows-print-spooler-service-vulnerability-closed
ED 21-03: Mitigate Pulse Connect Secure Product Vulnerabilities (Closed)		https://www.cisa.gov/news-events/directives/ed-21-03-mitigate-pulse-connect-secure-product-vulnerabilities-closed
ED 21-02: Mitigate Microsoft Exchange On-Premises Product Vulnerabilities (Closed)		https://www.cisa.gov/news-events/directives/ed-21-02-mitigate-microsoft-exchange-premises-product-vulnerabilities-closed
ED 21-01: Mitigate SolarWinds Orion Code Compromise (Closed)		https://www.cisa.gov/news-events/directives/ed-21-01-mitigate-solarwinds-orion-code-compromise-closed
ED 20-04: Mitigate Netlogon Elevation of Privilege Vulnerability from August 2020 Patch Tuesday (Closed)		https://www.cisa.gov/news-events/directives/ed-20-04-mitigate-netlogon-elevation-privilege-vulnerability-august-2020-patch-tuesday-closed
ED 20-03: Mitigate Windows DNS Server Remote Code Execution Vulnerability from July 2020 Patch Tuesday (Closed)		https://www.cisa.gov/news-events/directives/ed-20-03-mitigate-windows-dns-server-remote-code-execution-vulnerability-july-2020-patch-tuesday
ED 20-02: Mitigate Windows Vulnerabilities from January 2020 Patch Tuesday (Closed)		https://www.cisa.gov/news-events/directives/ed-20-02-mitigate-windows-vulnerabilities-january-2020-patch-tuesday-closed

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
Telegram Exposes Real Users IP Addresses, Bypassing Proxies on Android and iOS in 1-click	https://cybersecuritynews.com/one-click-telegram-flaw/
InvisibleJS Tool Hides Executable ES Modules in Empty Files Using Zero-Width Steganography	https://cybersecuritynews.com/invisiblejs-tool/
YARA-X 1.11.0 Released With a New Hash Function Warnings	https://cybersecuritynews.com/yara-x-1-11-0-released/
Google is Integrating Gemini AI with Gmail to Transform it into a Proactive Personal Assistant	https://cybersecuritynews.com/google-gemini-with-gmail/
New EDRStartupHinder Tool blocks antivirus and EDR services at startup on Windows 11 25H2 Defender	https://cybersecuritynews.com/edrstartuphinder-tool/
Instagram Confirms no System Breach and Fixed External Party Password Reset Issue	https://cybersecuritynews.com/instagram-confirms-no-system-breach/
Europol-Backed Operation Leads to 34 Arrests in Black Axe Crime Network Bust	https://cybersecuritynews.com/europol-backed-operation-leads-to-34-arrests-in-black-axe/
BreachForums Hack: Hackers Expose All User Records from Popular Dark Web Forum	https://cybersecuritynews.com/breachforums-hack/

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
Data Breach at Texas Gas Station Operator Exposes Info of 377,000+ Customers	https://cybersecuritynews.com/data-breach-at-texas-gas-station-operator-exposes/
Instagram Data Leak Exposes Sensitive Info of 17.5M Accounts [Updated]	https://cybersecuritynews.com/instagram-data-leak-exposes-sensitive-info-of-17-5m-accounts/
Threat actors Allegedly Claim Discord Dataset Containing 78,541,207 Files	https://cybersecuritynews.com/discord-breach-claim/

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
SAP Security Patch Day January 2026 – Patch for Critical Injection and RCE Vulnerabilities	https://cybersecuritynews.com/sap-security-patch-day-january-2026/
Critical ServiceNow Vulnerability Enables Privilege Escalation Via Unauthenticated User Impersonation	https://cybersecuritynews.com/servicenow-vulnerability/
CISA Warns of Gogs Path Traversal Vulnerability Exploited in Attacks	https://cybersecuritynews.com/cisa-gogs-path-traversal-vulnerability/
New Angular Vulnerability Enables an Attacker to Execute Malicious Payload	https://cybersecuritynews.com/angular-vulnerability/
100,000+ n8n Instances Exposed to Internet Vulnerable to RCE Attacks	https://cybersecuritynews.com/100000-n8n-instances-exposed/
Multiple Hikvision Vulnerabilities Let Attackers Cause Device Malfunction Using Crafted Packets	https://cybersecuritynews.com/multiple-hikvision-lan-vulnerabilities/
Hackers Infiltrated n8n's Community Node Ecosystem With a Weaponized npm Package	https://cybersecuritynews.com/n8ns-community-weaponized-npm-package/
Critical Apache Struts 2 Vulnerability Allow Attackers to Steal Sensitive Data	https://cybersecuritynews.com/critical-apache-struts-2-vulnerability/
Web3 Developer Environments Targeted by Social Engineering Campaign Leveraging Fake Interview Software	https://cybersecuritynews.com/web3-developer-environments-targeted-by-social-engineering-campaign/
Critical React Router Vulnerability Let Attackers Access or Modify Server Files	https://cybersecuritynews.com/react-router-vulnerability/
Critical InputPlumber Vulnerabilities Allows UI Input Injection and Denial-of-Service	https://cybersecuritynews.com/inputplumber-vulnerabilities/
Critical Zlib Vulnerability Let Attackers Trigger Buffer Overflow by Invoking untgz	https://cybersecuritynews.com/zlib-buffer-overflow-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

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
New VoidLink Cloud-Native Malware Attacking Linux Systems with Self-deletion Capabilities	https://cybersecuritynews.com/new-voidlink-cloud-native-malware/
DPRK's Remote Workers Generating $600M Using Identity Theft to Gain Access to Sensitive Systems	https://cybersecuritynews.com/dprks-remote-workers-generating-600m-using/
Hackers Leverage Browser-in-the-browser Tactic to Trick Facebook Users and Steal Logins	https://cybersecuritynews.com/hackers-leverage-browser-in-the-browser-tactic/
AsyncRAT Leveraging Cloudflare's Free-Tier Services to Mask Malicious Activities and Detection	https://cybersecuritynews.com/asyncrat-leveraging-cloudflares-free-tier-services/
Malicious Chrome Extension Steals Wallet Login Credentials and Enables Automated Trading	https://cybersecuritynews.com/malicious-chrome-extension-steals-wallet-login-credentials/
India Continues to Be the Top Target for Mobile Attacks with 38% Increase in Threats	https://cybersecuritynews.com/india-continues-to-be-the-top-target-for-mobile-attacks/
Cybercriminal Cryptocurrency Transactions Peaked in 2025 Following Nation-State Sanctions Evasion Moves	https://cybersecuritynews.com/cybercriminal-cryptocurrency-transactions-peaked/
ValleyRAT_S2 Attacking Organizations to Deploy Stealthy Malware and Extract Financial Details	https://cybersecuritynews.com/valleyrat_s2-attacking-organizations/
Beware of Weaponized Employee Performance Reports that Deploys Guloader Malware	https://cybersecuritynews.com/beware-of-weaponized-employee-performance-reports/
Everest Hacking Group Allegedly Claims Breach of Nissan Motors	https://cybersecuritynews.com/everest-hacking-group/
New Research Uncovers 28 Unique IP Addresses and 85 Domains Hosting Carding Markets	https://cybersecuritynews.com/new-research-uncovers-28-unique-ip-addresses/
New 'Penguin' Pig Butchering as a Service Selling PII, Stolen Accounts and Fraud Kits	https://cybersecuritynews.com/new-penguin-pig-butchering-as-a-service-selling-pii/
New MacSync Stealer Uses Signed macOS App to Evade Gatekeeper and Steal Data	https://cybersecuritynews.com/macsync-stealer-signed-macos-app-and-steal-data/
Phishing Campaign Uses Maduro Arrest Story to Deliver Backdoor Malware	https://cybersecuritynews.com/phishing-campaign-uses-maduro-arrest-deliver-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/