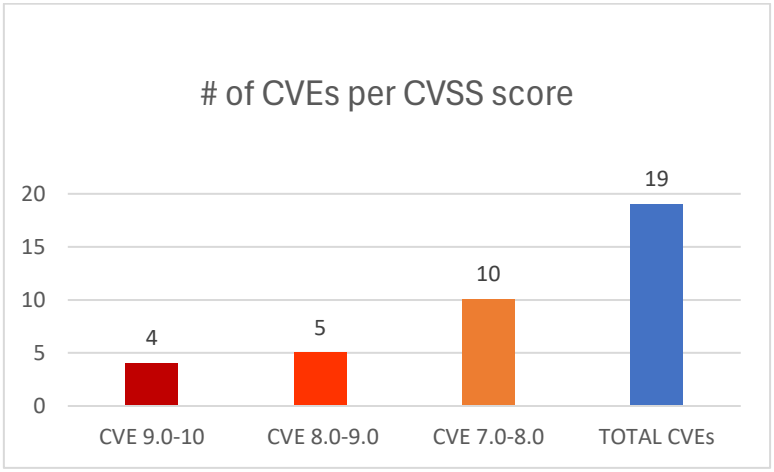
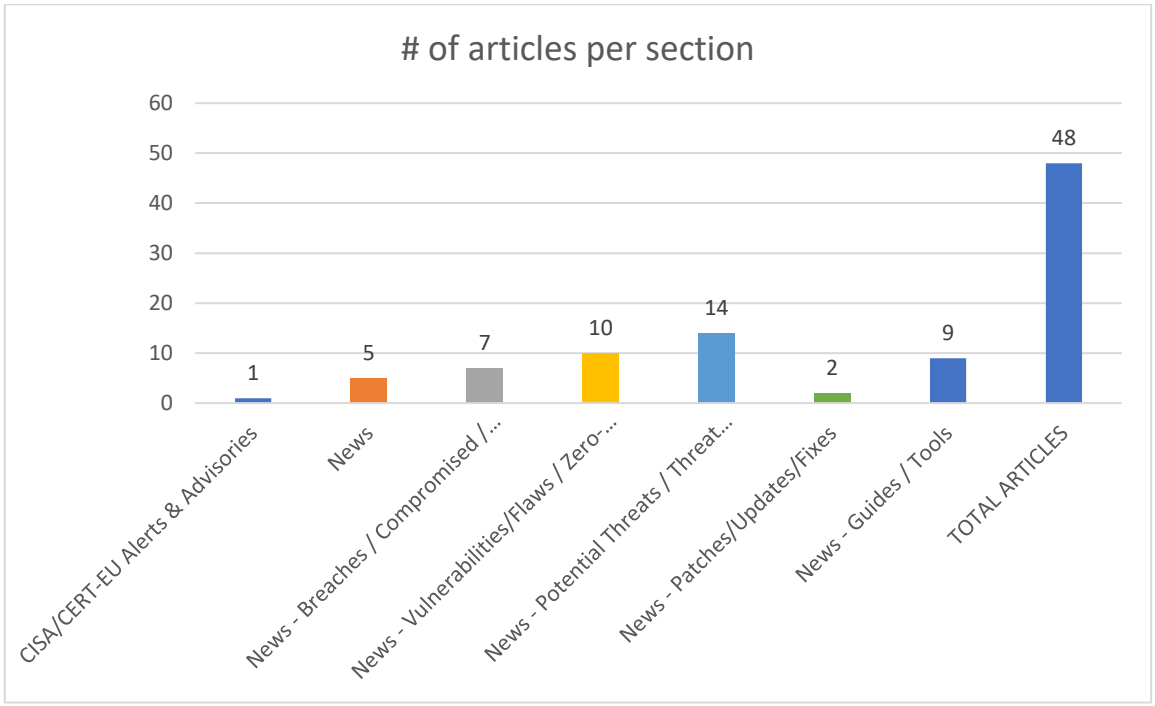
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 28/02/2026 - 03/03/2026





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)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2026-3422	9,8	U-Office Force	Deserialization of Untrusted Data		https://www.twcert.org.tw/en/cp-139-10743-9a952-2.html TWCERT/CC https://www.twcert.org.tw/tw/cp-132-10742-45b13-1.html
https://nvd.nist.gov/vuln/detail/CVE-2026-3000	9,8	IDExpert Windows Logon Agent	Download of Code Without Integrity Check		https://www.changingtec.com/news_detail.jsp?item_id=348 TWCERT/CC https://www.twcert.org.tw/en/cp-139-10741-daed4-2.html TWCERT/CC https://www.twcert.org.tw/tw/cp-132-10740-b2eb2-1.html
https://nvd.nist.gov/vuln/detail/CVE-2026-27966	9,8	Langflow	Improper Control of Generation of Code ('Code Injection')	Prior to version 1.8.0	https://github.com/langflow-ai/langflow/commit/d8c6480daa17b2f2af0b5470cdf5c3d28dc9e508 GitHub, Inc. Patch https://github.com/langflow-ai/langflow/security/advisories/GHSA-3645-fxcv-hqr4
https://nvd.nist.gov/vuln/detail/CVE-2026-27647	9,8	The WebSocket	Insufficient Session Expiration		https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-057-08.json ICS-CERT Third Party Advisory https://www.cisa.gov/news-events/ics-advisories/icsa-26-057-08 ICS-CERT Third Party Advisory VDB Entry https://www.mobility46.se/en/contact-us
https://nvd.nist.gov/vuln/detail/CVE-2026-3400	8,8	Tenda AC15	Stack-based Buffer Overflow	up to 15.13.07.13	https://vuldb.com/?ctiid.348295 VulDB https://vuldb.com/?id.348295 VulDB https://vuldb.com/?submit.760109 VulDB https://www.tenda.com.cn/ VulDB

					https://www.yuque.com/ba1ma0-an29k/nnxoap/tzg68iadbmqx6esm?singleDoc#
https://nvd.nist.gov/vuln/detail/CVE-2026-27969	8,8	Vitess	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Prior to versions 23.0.3 and 22.0.4	https://github.com/vitessio/vitess/commit/c565cab615bc962bda061dcd645aa7506c59ca4a GitHub, Inc. Patch https://github.com/vitessio/vitess/pull/19470 GitHub, Inc. Issue Tracking Patch https://github.com/vitessio/vitess/security/advisories/GHSA-r492-hjgh-c9gw
https://nvd.nist.gov/vuln/detail/CVE-2026-28363	8,8	OpenClaw	Incomplete List of Disallowed Inputs	before 2026.2.23	https://github.com/openclaw/openclaw/security/advisories/GHSA-3c6h-g97w-fg78
https://nvd.nist.gov/vuln/detail/CVE-2026-20764	8,8	XWEB Pro	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	1.12.1 and prior	https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-057-10.json ICS-CERT Third Party Advisory https://webapps.copeland.com/Dixell/Pages/SystemSoftwareUpdate ICS-CERT Product https://www.cisa.gov/news-events/ics-advisories/icsa-26-057
https://nvd.nist.gov/vuln/detail/CVE-2026-28562	8,2	wpForo	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	2.4.14	https://wordpress.org/plugins/wpforo/ VulnCheck https://wordpress.org/plugins/wpforo/#developers VulnCheck https://www.vulncheck.com/advisories/wpforo-sql-injection-via-topics-order-by-parameter
https://nvd.nist.gov/vuln/detail/CVE-2026-28364	7,9	In Ocaml	Buffer Over-read	before 4.14.3 and 5.x before 5.4.1	https://github.com/ocaml/security-advisories/blob/generated-osv/2026/OSEC-2026-01.json MITRE https://osv.dev/vulnerability/OSEC-2026-01

https://nvd.nist.gov/vuln/detail/CVE-2026-2471	7,5	The WP Mail Logging plugin for WordPress	Deserialization of Untrusted Data	up to, and including, 1.15.0	https://plugins.trac.wordpress.org/browser/wp-mail-logging/tags/1.15.0/lib/vendor/brandonwamboldt/wp-orm/src/BaseModel.php#L39 Wordfence https://plugins.trac.wordpress.org/browser/wp-mail-logging/tags/1.15.0/src/Renderer/WPML_MailRenderer_AJAX_Handler.php#L100 Wordfence https://plugins.trac.wordpress.org/browser/wp-mail-logging/tags/1.15.0/src/WPML_Plugin.php#L553 Wordfence https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3464813%40wp-mail-logging&old=3358334%40wp-mail-logging&sfp_email=&sfph_mail= Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/10e4c52d-c82f-4393-9a56-5714b3a108d1?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-13673	7,5	The Tutor LMS	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	all versions up to, and including, 3.9.6	https://plugins.trac.wordpress.org/changeset/3469242/tutor Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/007df869-dacb-4b0a-9c98-50586934cdab?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-27449	7,5	Umbraco Engage	Improper Access Control	prior to versions 16.2.1 and 17.1.1	https://github.com/umbraco/Umbraco.Engage.Issues/security/advisories/GHSA-86vq-ccwf-rm62
https://nvd.nist.gov/vuln/detail/CVE-2026-2428	7,5	The Fluent Forms Pro Add On Pack plugin for WordPress	Insufficient Verification of Data Authenticity	all versions up to, and including, 6.1.17	https://fluentforms.com/docs/changelog/#2-toc-title Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/e5c62e54-da06-4b44-ba70-63065e664b0d?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2026-3413	7,3	University Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/JXBbozaihuang/vuln-research/issues/1 VulDB https://itsourcecode.com/ VulDB https://vuldb.com/?ctiid.348308 VulDB https://vuldb.com/?id.348308 VulDB https://vuldb.com/?submit.764004
https://nvd.nist.gov/vuln/detail/CVE-2026-3410	7,3	Society Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
https://nvd.nist.gov/vuln/detail/CVE-2026-3409	7,3	eosphoros-ai db-gpt	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	0.7.5	https://gist.github.com/YLChen-007/d2799d8b2077e50658f12a45bcae9b70 VulDB https://vuldb.com/?ctiid.348304 VulDB https://vuldb.com/?id.348304 VulDB https://vuldb.com/?submit.763745
https://nvd.nist.gov/vuln/detail/CVE-2026-3406	7,3	Online Art Gallery Shop	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/ubfbuz3/cve/issues/55 VulDB https://vuldb.com/?ctiid.348301 VulDB https://vuldb.com/?id.348301 VulDB https://vuldb.com/?submit.763740

https://nvd.nist.gov/vuln/detail/CVE-2026-3395	7,3	MaxSite CMS	Improper Control of Generation of Code ('Code Injection')	up to 109.1	https://github.com/maxsite/cms/ VulDB https://github.com/maxsite/cms/commit/08937a3c5d672a242d68f53e9fccf8a748820ef3 VulDB https://vuldb.com/?ctiid.348281 VulDB https://vuldb.com/?id.348281 VulDB https://vuldb.com/?submit.762169

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 Two Known Exploited Vulnerabilities to Catalog	▪ **CVE-2026-21385 Qualcomm Multiple Chipsets Memory Corruption Vulnerability** ▪ **CVE-2026-22719 Broadcom VMware Aria Operations Command Injection Vulnerability**	**https://www.cisa.gov/news-events/alerts/2026/03/03/cisa-adds-two-known-exploited-vulnerabilities-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
Trump Bans Anthropic AI in Federal Agencies — Pentagon Flags Claude as Security Risk	https://cybersecuritynews.com/trump-bans-anthropic-ai/
Leaked Database Sheds Light on Iranian Crypto Sanctions Evasion	https://www.infosecurity-magazine.com/news/iranian-crypto-leaked-database/
Iranian Cyber Threat Actor Targets Iraqi Government Officials in AI-Powered Campaign	https://www.infosecurity-magazine.com/news/iran-cyber-threat-actor-iraq/
Chrome Unveils Plan For Quantum-Safe HTTPS Certificates	https://www.infosecurity-magazine.com/news/chrome-quantum-safe-https/
Epic Fury/Roaring Lion Sparks Escalating Cyber Conflict as Iran Goes Offline, Hacktivists Step Up Retaliation	https://cybersecuritynews.com/epic-fury-roaring-lion-sparks-escalating-cyber-conflict/

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
Thousands of Public Google Cloud API Keys Exposed with Gemini Access After API Enablement	https://thehackernews.com/2026/02/thousands-of-public-google-cloud-api.html
AWS Power Outage in Middle East Triggers Major Disruption to EC2 and Networking Services	https://cybersecuritynews.com/aws-power-outage/
Hacked Prayer App Used as Cyber Weapon During US-Israel Strikes on Iran	https://cybersecuritynews.com/hacked-prayer-app/
ClawJacked attack let malicious websites hijack OpenClaw to steal data	https://www.bleepingcomputer.com/news/security/clawjacked-attack-let-malicious-websites-hijack-openclaw-to-steal-data/
$4.8M in crypto stolen after Korean tax agency exposes wallet seed	https://www.bleepingcomputer.com/news/security/48m-in-crypto-stolen-after-korean-tax-agency-exposes-wallet-seed/?&web_view=true
University of Hawai'i Cancer Center confirms data leak following ransomware attack	https://therecord.media/university-of-hawaii-ransomware-data-breach?&web_view=true
LexisNexis Data Breach — Threat Actor Allegedly Claims 2.04 GB Stolen	https://cybersecuritynews.com/lexisnexis-data-breach/

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
ClawJacked Flaw Lets Malicious Sites Hijack Local OpenClaw AI Agents via WebSocket	https://thehackernews.com/2026/02/clawjacked-flaw-lets-malicious-sites.html
OpenClaw 0-Click Vulnerability Allows Malicious Websites to Hijack Developer AI Agents	https://cybersecuritynews.com/openclaw-0-click-vulnerability/
Google Confirms CVE-2026-21385 in Qualcomm Android Component Exploited	https://thehackernews.com/2026/03/google-confirms-cve-2026-21385-in.html
New Chrome Vulnerability Let Malicious Extensions Escalate Privileges via Gemini Panel	https://thehackernews.com/2026/03/new-chrome-vulnerability-let-malicious.html
APT28 Tied to CVE-2026-21513 MSHTML 0-Day Exploited Before Feb 2026 Patch Tuesday	https://thehackernews.com/2026/03/apt28-tied-to-cve-2026-21513-mshtml-0.html
Vulnerability in MS-Agent AI Framework Can Allow Full System Compromise	https://www.securityweek.com/vulnerability-in-ms-agent-ai-framework-can-allow-full-system-compromise/
Vulnerability Allowed Hijacking Chrome's Gemini Live AI Assistant	https://www.securityweek.com/vulnerability-allowed-hijacking-chromes-gemini-live-ai-assistant/

CISA flags VMware Aria Operations RCE flaw as exploited in attacks	https://www.bleepingcomputer.com/news/security/cisa-flags-vmware-aria-operations-rce-flaw-as-exploited-in-attacks/
Zerobot Malware Exploiting Tenda Command Injection Vulnerabilities to Deploy Malware	https://cybersecuritynews.com/zerobot-malware-exploiting-tenda-command/
Langflow's AI CSV Agent Vulnerability Allows Remote Code Execution Attacks	https://cybersecuritynews.com/langflows-ai-csv-agent-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
Metasploit Adds New Modules Targeting Linux RC4, BeyondTrust, and Registry Persistence	https://cybersecuritynews.com/metasploit-adds-new-modules-targeting-linux-rc4/
Android Update Patches Exploited Qualcomm Zero-Day	https://www.securityweek.com/android-update-patches-exploited-qualcomm-zero-day/

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
Hackers Abuse Windows File Explorer and WebDAV for Stealthy Malware Delivery	https://cybersecuritynews.com/hackers-abuse-windows-file-explorer-and-webdav/
Phishing Schemes Abuse .arpa TLD and IPv6 Tunnels to Evade Detection	**https://cybersecuritynews.com/phishing-schemes-abuse-arpa-tld-and-ipv6-tunnels/**
Pixel Perfect Extension Abuse Enables Covert Script Injection and Security Header Removal	https://cybersecuritynews.com/pixel-perfect-extension-abuse-enables-covert-script-injection/
Indian APT 'Sloppy Lemming' Targets Defense, Critical Infrastructure	https://www.darkreading.com/threat-intelligence/india-apt-sloppy-lemming-defense-critical-infrastructure
Israel: RedAlert Spyware Campaign Exploits Wartime Panic With Trojanized App	https://www.infosecurity-magazine.com/news/redalert-israel-spyware-campaign/
AI and Deepfakes Supercharge Sophisticated Cyber-Attacks, Says Cloudflare	https://www.infosecurity-magazine.com/news/ai-deepfakes-supercharge/
SloppyLemming Espionage Campaign Uses BurrowShell Backdoor and Rust RAT to Hit Pakistan and Bangladesh Targets	https://cybersecuritynews.com/sloppylemming-espionage-campaign-uses-burrowshell-backdoor/
Malvertising Threat Actor 'D-Shortiez' Abuses WebKit Back-Button Hijack in Forced-Redirect Browser Campaign	https://cybersecuritynews.com/malvertising-threat-actor-d-shortiez-abuses-webkit-back-button/
Microsoft Warns of New Phishing Attack Exploiting OAuth in Entra ID to Evade Detection	https://cybersecuritynews.com/phishing-attack-exploiting-oauth/
Hackers Leverage Telegram for Initial Access to Corporate VPN, RDP, and Cloud Environments	https://cybersecuritynews.com/hackers-leverage-telegram-for-initial-access/
Hackerbot-Claw Bot Attacks Microsoft and DataDog via GitHub Actions CI/CD Misconfiguration	https://cybersecuritynews.com/hackerbot-claw-bot-attacks-microsoft-and-datadog/

Threat Actors Exploit OpenVSX Aqua Trivy with Malicious AI Prompts to Hijack Local Coding Tools	https://cybersecuritynews.com/threat-actors-exploit-openvsx-aqua-trivy/
Hackers Leveraged CyberStrikeAI Tool to Breach Fortinet FortiGate Devices	https://cybersecuritynews.com/cyberstrikeai-tool-breach-fortigate-devices/
Malvertising Campaign Delivers AMOS 'malext' macOS Infostealer via Fake Text-Sharing Lures	https://cybersecuritynews.com/malvertising-campaign-delivers-amos-malext-macos-infostealer/

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/**
Splunk Releases Guide to Detect Remote Employment Fraud Within Your Organization	https://cybersecuritynews.com/detect-remote-employment-fraud/
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/
Top 10 Best Exposure Management Tools In 2026	https://cybersecuritynews.com/best-exposure-management-tools/
NETREAPER Offensive Security Toolkit That Wraps 70+ Penetration Testing Tools	https://cybersecuritynews.com/netreaper-offensive-security-toolkit/
GitLab Security Best Practices Cheat Sheet	https://thehackernews.uk/gitlab-security-tips
False Negatives Are a New SOC Headache. Here's the Fast Way to Fix It	https://cybersecuritynews.com/false-negatives-are-a-new-soc-headache-heres-the-fast-way-to-fix-it/
PentAGI – Automated AI-Powered Penetration Testing Tool that Integrates 20+ Security Tools	https://cybersecuritynews.com/pentagi-penetration-testing-tool/

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/