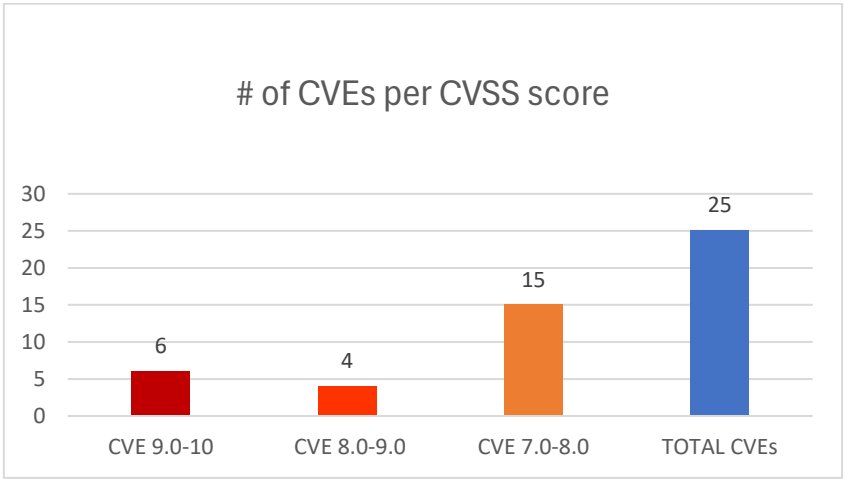
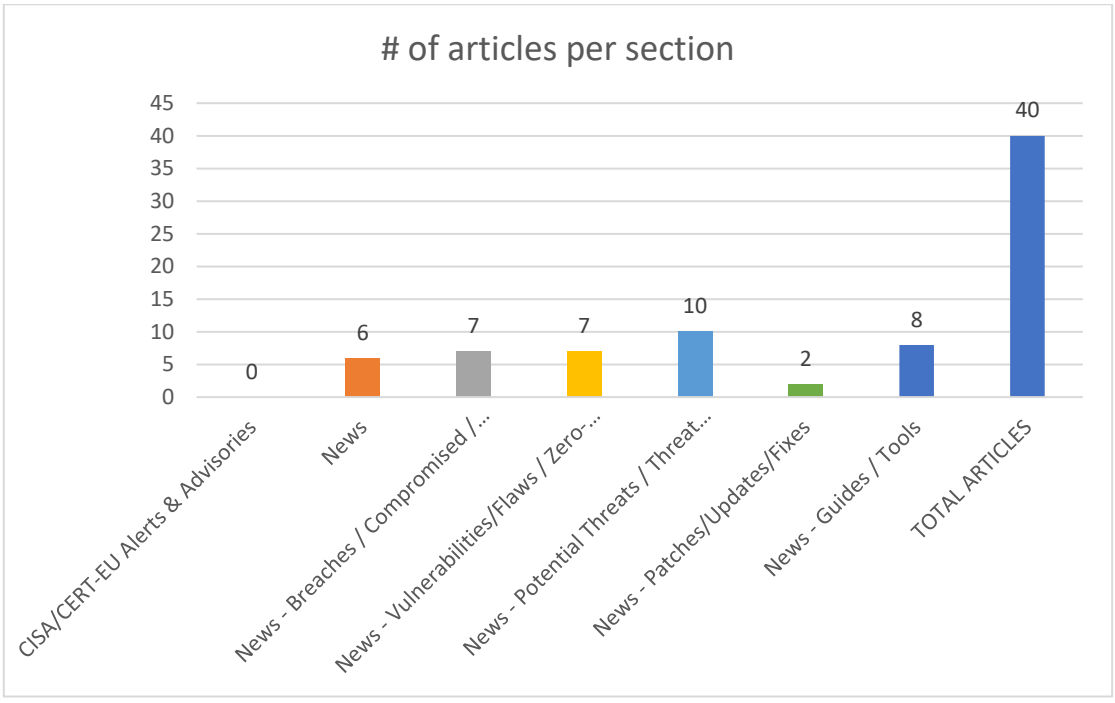
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 07/02/2026 - 10/02/2026





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-2026-0488	9,9	SAP CRM and SAP S/4HANA	Missing Authorization		https://me.sap.com/notes/3697099 SAP SE https://url.sap/sapsecuritypatchday
https://nvd.nist.gov/vuln/detail/CVE-2026-22906	9,8	AES-ECB	Use of Hard-coded Cryptographic Key		https://certvde.com/de/advisories/VDE-2026-004
https://nvd.nist.gov/vuln/detail/CVE-2026-2096	9,8	Agentflow	Authentication Bypass Using an Alternate Path or Channel		https://forum.flowring.com/post/view?bid=72&id=45611&tpg=1&ppg=1&sty=1#45939 TWCERT/CC https://www.twcert.org.tw/en/cp-139-10700-3534d-2.html TWCERT/CC https://www.twcert.org.tw/tw/cp-132-10699-49c0b-1.html
https://nvd.nist.gov/vuln/detail/CVE-2026-25848	9,1	In JetBrains Hub	Missing Authentication for Critical Function	before 2025.3.119807	https://www.jetbrains.com/privacy-security/issues-fixed/
https://nvd.nist.gov/vuln/detail/CVE-2026-25057	9,1	MarkUs	Relative Path Traversal	Prior to 2.9.1	https://github.com/MarkUsProject/Markus/commit/0ca002a1f0071c7a00dbb2ed34fede57323c5dc7 GitHub, Inc. https://github.com/MarkUsProject/Markus/releases/tag/v2.9.1 GitHub, Inc. https://github.com/MarkUsProject/Markus/security/advisories/GHSA-mccg-p332-252h
https://nvd.nist.gov/vuln/detail/CVE-2026-25881	9,0	SandboxJS	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	Prior to 0.8.31	https://github.com/nyariv/SandboxJS/commit/f369f8db26649f212a6a9a2e7a1624cb2f705b53 GitHub, Inc.

					https://github.com/nyariv/SandboxJS/security/advisories/GHSA-ww7g-4gwx-m7wj
https://nvd.nist.gov/vuln/detail/CVE-2026-25807	8,8	ZAI Shell	Improper Control of Generation of Code ('Code Injection')	Prior to 9.0.3	https://github.com/TaklaXBR/zai-shell/commit/a4ea8525d912f55d6e2f09b2869966c52d189a4a GitHub, Inc. https://github.com/TaklaXBR/zai-shell/releases/tag/v9.0.3 GitHub, Inc. https://github.com/TaklaXBR/zai-shell/security/advisories/GHSA-6pjj-r955-34rr
https://nvd.nist.gov/vuln/detail/CVE-2026-25761	8,8	Super-linter	Improper Neutralization of Special Elements used in a Command ('Command Injection')	From 6.0.0 to 8.3.0	https://github.com/super-linter/super-linter/releases/tag/v8.3.1 GitHub, Inc. https://github.com/super-linter/super-linter/security/advisories/GHSA-r79c-pqj3-577x
https://nvd.nist.gov/vuln/detail/CVE-2026-25847	8,2	JetBrains PyCharm	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	before 2025.3.2	https://www.jetbrains.com/privacy-security/issues-fixed/
https://nvd.nist.gov/vuln/detail/CVE-2026-25890	8,1	File Browser	Incorrect Authorization	Prior to 2.57.1	https://github.com/filebrowser/filebrowser/commit/489af403a19057f6b6b4b1dc0e48cbb26a202ef9 GitHub, Inc. https://github.com/filebrowser/filebrowser/releases/tag/v2.57.1 GitHub, Inc. https://github.com/filebrowser/filebrowser/security/advisories/GHSA-4mh3-h929-w968
https://nvd.nist.gov/vuln/detail/CVE-2026-25931	7,8	vscode-spell-checker	Reliance on Untrusted Inputs in a Security Decision	Prior to v4.5.4	https://drive.google.com/file/d/1mT4SOkkHSHU6NFfKwekysydAd3FUAC6K/view?usp=sharing GitHub, Inc. https://github.com/streetsidesoftware/vscode-spell-checker/commit/f39af9a3a6f2a939a57171a24161ed735d41c575 GitHub, Inc.

					https://github.com/streetsidesoftware/vscode-spell-checker/releases/tag/code-spell-checker-v4.5.4 GitHub, Inc. https://github.com/streetsidesoftware/vscode-spell-checker/security/advisories/GHSA-mggq-68mr-58vj
https://nvd.nist.gov/vuln/detail/CVE-2026-25925	7,8	PowerDocu	Deserialization of Untrusted Data	Prior to 2.4.0	https://github.com/modery/PowerDocu/releases/tag/v-2.4.0 GitHub, Inc. https://github.com/modery/PowerDocu/security/advisories/GHSA-m8j2-5jr7-2jpw
https://nvd.nist.gov/vuln/detail/CVE-2025-11547	7,8	AXIS Camera Station Pro	Insertion of Sensitive Information into Log File		https://www.axis.com/dam/public/permalink/253485/cve-2025-11547pdf-en-US_253485.pdf?noS3=1
https://nvd.nist.gov/vuln/detail/CVE-2026-25958	7,7	Cube	Reliance on Untrusted Inputs in a Security Decision	From 0.27.19 to before 1.5.13, 1.4.2, and 1.0.14	https://github.com/cube-js/cube/security/advisories/GHSA-v226-32c7-x2v7
https://nvd.nist.gov/vuln/detail/CVE-2026-24322	7,7	SAP Solution Tools Plug-In (ST-PI)	Missing Authorization		https://me.sap.com/notes/3705882 SAP SE https://url.sap/sapsecuritypatchday
https://nvd.nist.gov/vuln/detail/CVE-2026-25961	7,5	SumatraPDF	Improper Certificate Validation	In 3.5.0 through 3.5.2	https://github.com/sumatrapdfreader/sumatrapdf/security/advisories/GHSA-xpm2-rr5m-x96q
https://nvd.nist.gov/vuln/detail/CVE-2026-25892	7,5	Adminer	Improper Input Validation	Adminer v5.4.1	https://github.com/vrana/adminer/commit/21d3a3150388677b18647d68aec93b7850e457d3 GitHub, Inc. https://github.com/vrana/adminer/releases/tag/v5.4.2 GitHub, Inc. https://github.com/vrana/adminer/security/advisories/GHSA-q4f2-39gr-45jh
https://nvd.nist.gov/vuln/detail/CVE-2026-25808	7,5	Hollo	Missing Authorization	Prior to 0.6.20 and 0.7.2	https://github.com/fedify-dev/hollo/commit/329969c502ef092d5c3f9c2c20421c34f4ff0f0e GitHub, Inc.

					https://github.com/fedify-dev/hollo/releases/tag/0.6.20 GitHub, Inc. https://github.com/fedify-dev/hollo/releases/tag/0.7.2 GitHub, Inc. https://github.com/fedify-dev/hollo/security/advisories/GHSA-6r2w-3pcj-v4v5
https://nvd.nist.gov/vuln/detail/CVE-2026-25791	7,5	Sliver	Uncontrolled Resource Consumption	Prior to 1.7.0	https://github.com/BishopFox/sliver/releases/tag/v1.7.0 GitHub, Inc. https://github.com/BishopFox/sliver/security/advisories/GHSA-wxrw-gvg8-fqjp
https://nvd.nist.gov/vuln/detail/CVE-2026-25639	7,5	Axios	Improper Check for Unusual or Exceptional Conditions	Prior to 1.13.5	https://github.com/axios/axios/commit/28c721588c7a77e7503d0a434e016f852c597b57 GitHub, Inc. https://github.com/axios/axios/releases/tag/v1.13.5 GitHub, Inc. https://github.com/axios/axios/security/advisories/GHSA-43fc-jf86-j433
https://nvd.nist.gov/vuln/detail/CVE-2026-25231	7,5	FileRise	Improper Access Control	prior to 3.3.0	https://github.com/error311/FileRise/releases/tag/v3.3.0 GitHub, Inc. https://github.com/error311/FileRise/security/advisories/GHSA-hv99-77cw-hvpr
https://nvd.nist.gov/vuln/detail/CVE-2026-25639	7,5	Axios	Improper Check for Unusual or Exceptional Conditions	Prior to 1.13.5	https://github.com/axios/axios/commit/28c721588c7a77e7503d0a434e016f852c597b57 GitHub, Inc. https://github.com/axios/axios/releases/tag/v1.13.5 GitHub, Inc. https://github.com/axios/axios/security/advisories/GHSA-43fc-jf86-j433
https://nvd.nist.gov/vuln/detail/CVE-2026-25478	7,4	Litestar	Permissive Cross-domain Policy with Untrusted Domains	Prior to 2.20.0	https://docs.litestar.dev/2/release-notes/changelog.html#2.20.0 GitHub, Inc. https://github.com/litestar-org/litestar/commit/eb87703b309efcc0d1b087dcb12784e76b003d5a GitHub, Inc.

					https://github.com/litestar-org/litestar/releases/tag/v2.20.0 GitHub, Inc. https://github.com/litestar-org/litestar/security/advisories/GHSA-2p2x-hpg8-cqp2
https://nvd.nist.gov/vuln/detail/CVE-2026-2260	7,2	D-Link DCS-931L	Improper Neutralization of Special Elements used in a Command ('Command Injection')	up to 1.13.0	https://github.com/cha0yang1/CVE/blob/main/DLinkRce.md VulDB https://github.com/cha0yang1/CVE/blob/main/DLinkRce.md#poc VulDB https://vuldb.com/?ctiid.345007 VulDB https://vuldb.com/?id.345007 VulDB https://vuldb.com/?submit.753398 VulDB https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-2191	7,2	Tenda AC9	Stack-based Buffer Overflow	15.03.06.42_multi	https://github.com/glkfc/IoT-Vulnerability/blob/main/Tenda/tenda3.md VulDB https://vuldb.com/?ctiid.344894 VulDB https://vuldb.com/?id.344894 VulDB https://vuldb.com/?submit.749800 VulDB https://www.tenda.com.cn/

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
OpenClaw Integrates VirusTotal Scanning to Detect Malicious ClawHub Skills	https://thehackernews.com/2026/02/openclaw-integrates-virustotal-scanning.html
UK Construction Firm Hit by Prometei Botnet Hiding in Windows Server	https://hackread.com/uk-construction-firm-prometei-botnet-windows-server/?&web_view=true
Ransomware Detection With Windows Minifilter by Intercepting File Filter and Change Events	https://cybersecuritynews.com/ransomware-detection-with-windows-minifilter/
New Paper and Tool Help Security Teams Move Beyond Blind Reliance on CISA's KEV Catalog	https://www.securityweek.com/new-paper-and-tool-help-security-teams-move-beyond-blind-reliance-on-cisas-kev-catalog/
Augustus – Open-source LLM Vulnerability Scanner With 210+ Attacks Across 28 LLM Providers	https://cybersecuritynews.com/augustus-llm-vulnerability-scanner/
DPRK IT Workers Impersonating Individuals Using Real LinkedIn Accounts to Apply for Remote Roles	https://cybersecuritynews.com/dprk-it-workers-impersonating-individuals/

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
Dutch Authorities Confirm Ivanti Zero-Day Exploit Exposed Employee Contact Data	https://thehackernews.com/2026/02/dutch-authorities-confirm-ivanti-zero.html
Birmingham mental health authority warns 30,000+ people of data breach that leaked SSNs and medical info	https://www.comparitech.com/news/birmingham-mental-health-authority-warns-30000-people-of-data-breach-that-leaked-ssns-and-medical-info/?&web_view=true
Flickr emails users about data breach, pins it on third party	https://www.theregister.com/2026/02/06/flickr_emails_users_about_data_breach/?&web_view=true
Payments platform BridgePay confirms ransomware attack behind outage	https://www.bleepingcomputer.com/news/security/payments-platform-bridgepay-confirms-ransomware-attack-behind-outage/?&web_view=true
Warlock Gang Breaches SmarterTools Via SmarterMail Bugs	https://www.darkreading.com/application-security/warlock-gang-breaches-smartertools-smartermail-bugs
AI Chat App Exposes 300 Million Messages from 25 Million Users	https://cybersecuritynews.com/ai-chat-app-exposes-messages/
European Governments Breached in Zero-Day Attacks Targeting Ivanti	https://www.infosecurity-magazine.com/news/european-governments-zeroday/

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 SmarterMail Vulnerability Exploited in Ransomware Attacks	https://www.securityweek.com/critical-smartermail-vulnerability-exploited-in-ransomware-attacks/
Critical FortiClientEMS Vulnerability Let Attackers Execute Malicious Code Remotely	https://cybersecuritynews.com/forticlientems-rce-vulnerability/
New RecoverIt Tool Exploits Windows Service Failure Recovery Functions to Execute Payload	https://cybersecuritynews.com/recoverit-tool/
Hackers Actively Exploiting SolarWinds Web Help Desk RCE Vulnerability to Deploy Custom Tools	https://cybersecuritynews.com/solarwinds-vulnerability-actively-exploited/
Recent SolarWinds Flaws Potentially Exploited as Zero-Days	https://www.securityweek.com/recent-solarwinds-flaws-potentially-exploited-as-zero-days/
15,200 OpenClaw Control Panels with Full System Access Exposed to the Internet	https://cybersecuritynews.com/openclaw-control-panels-exposed/
New Zero-Click Flaw in Claude Desktop Extensions, Anthropic Declines Fix	https://www.infosecurity-magazine.com/news/zeroclick-flaw-claude-dxt/

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
BeyondTrust Fixes Critical Pre-Auth RCE Vulnerability in Remote Support and PRA	https://thehackernews.com/2026/02/beyondtrust-fixes-critical-pre-auth-rce.html
Fortinet Patches Critical SQLi Flaw Enabling Unauthenticated Code Execution	https://thehackernews.com/2026/02/fortinet-patches-critical-sqli-flaw.html

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
TeamPCP Worm Exploits Cloud Infrastructure to Build Criminal Infrastructure	https://thehackernews.com/2026/02/teampcp-worm-exploits-cloud.html
New Telegram Phishing Attack Abuses Authentication Workflows to Obtain Full Authorized User Sessions	**https://cybersecuritynews.com/new-telegram-phishing-attack-abuses-authentication-workflows/**
Black Basta Ransomware Actors Embeds BYOVD Defense Evasion Component with Ransomware Payload Itself	https://cybersecuritynews.com/black-basta-ransomware-actors-embeds-byovd/

Hackers Attacking IT & OSINT Professionals with New PyStoreRAT to Gain Remote Access	https://cybersecuritynews.com/hackers-attacking-it-osint-professionals/
Beware of Apple Pay Phishing Attack that Aims to Steal Your Payment Details	https://cybersecuritynews.com/beware-of-apple-pay-phishing-attack/
'Reynolds' Bundles BYOVD With Ransomware Payload	https://www.darkreading.com/threat-intelligence/black-basta-bundles-byovd-ransomware-payload
TeamPCP Turns Cloud Infrastructure into Crime Bots	https://www.darkreading.com/cloud-security/teampcp-cloud-infrastructure-crime-bots
Bloody Wolf Hackers Attacking Organizations to Deploy NetSupport RAT and Gain Remote Access	https://cybersecuritynews.com/bloody-wolf-hackers-attacking-organizations/
Threat Actor Claims Leak of Cybercrime-Focused AI Platform WormGPT Database	https://cybersecuritynews.com/wormgpt-database-leak/
GuLoader Uses Polymorphic Code and Trusted Cloud Hosting to Evade Reputation-Based Defenses	https://cybersecuritynews.com/guloader-uses-polymorphic-code-and-trusted-cloud-hosting/

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/

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/