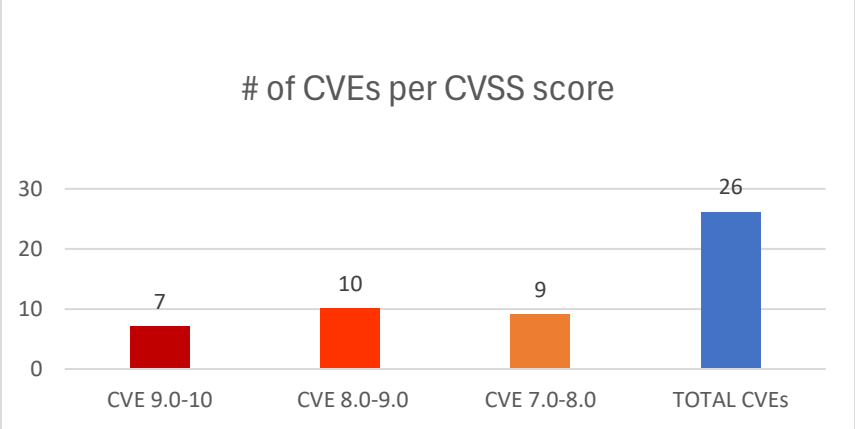
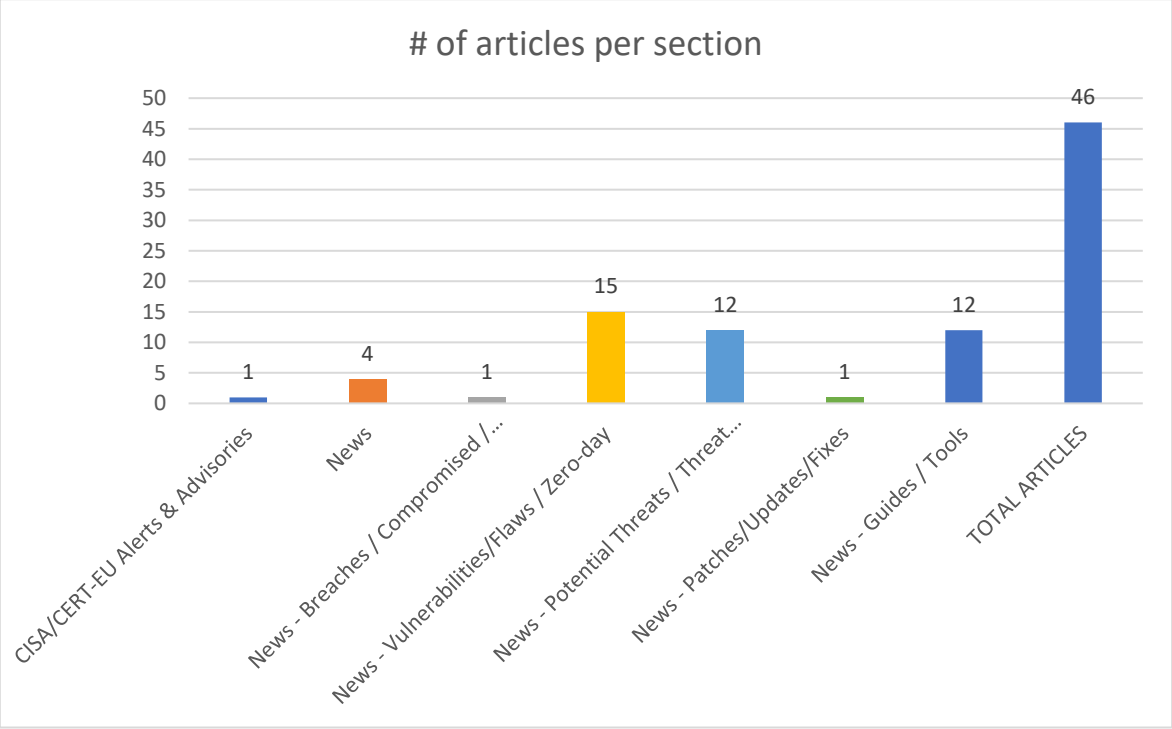
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 30/05/2026 - 02/06/2026





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-2026-40965	10,0	Cloud Foundry UAA	Exposure of Sensitive Information to an Unauthorized Actor	versions v76.12.0 through v78.12.0	https://www.cloudfoundry.org/blog/cve-2026-40965-uaa-ec-private-key-disclosure/
https://nvd.nist.gov/vuln/detail/CVE-2026-8206	9,8	The Kirki – Freeform Page Builder, Website Builder & Customizer plugin for WordPress	Improper Privilege Management	all versions 6.0.0 to 6.0.6	https://plugins.trac.wordpress.org/browser/kirki/tags/6.0.4/ComponentLibrary/controller/CompLibFormHandler.php#L330
https://nvd.nist.gov/vuln/detail/CVE-2018-25427	9,8	Arm Whois	Stack-based Buffer Overflow	3.11	http://www.armcode.com/ VulnCheck http://www.armcode.com/downloads/arm-whois.exe VulnCheck https://www.exploit-db.com/exploits/45796 VulnCheck https://www.vulncheck.com/advisories/arm-whois-buffer-overflow-via-seh-overwrite
https://nvd.nist.gov/vuln/detail/CVE-2026-44825	9,8	Apache Solr	Insecure Default Initialization of Resource	9.4.0 through 9.10.1 and 10.0.0	http://www.openwall.com/lists/oss-security/2026/05/29/6 CVE Mailing List Third Party Advisory https://lists.apache.org/thread/5xg6xr99glocp3zsg9ht2zlbwl-rst7ch
https://nvd.nist.gov/vuln/detail/CVE-2018-25412	9,8	Delta Sql	Missing Authentication for Critical Function	1.8.2	http://deltasql.sourceforge.net/ VulnCheck http://deltasql.sourceforge.net/deltasql/ VulnCheck https://sourceforge.net/projects/deltasql/files/latest/download VulnCheck https://www.exploit-db.com/exploits/45685 VulnCheck https://www.vulncheck.com/advisories/delta-sql-arbitrary-file-upload-via-docs-upload-php

https://nvd.nist.gov/vuln/detail/CVE-2026-44211	9,6	Cline	Missing Authentication for Critical Function	2.13.0 and prior	https://github.com/cline/cline/security/advisories/GHSA-5c57-rqjx-35g2
https://nvd.nist.gov/vuln/detail/CVE-2026-48188	9,1	OTRS or ((OTRS)) Community Edition	Improper Input Validation	OTRS: * 7.0.X * 8.0.X * 2023.X * 2024.X * 2025.X * 2026.X before 2026.4.X *	https://otrs.com/release-notes/otrs-security-advisory-2026-02/
https://nvd.nist.gov/vuln/detail/CVE-2026-9614	8,8	Ivanti Neurons for ITSM	Improper Access Control		https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Neurons-for-ITSM-CVE-2026-9614
https://nvd.nist.gov/vuln/detail/CVE-2026-43623	8,8	microtar	Stack-based Buffer Overflow	through 0.1.0	https://github.com/rxi/microtar/issues/28 VulnCheck https://github.com/rxi/microtar/issues/29 VulnCheck https://github.com/rxi/microtar/issues/30 VulnCheck https://www.vulncheck.com/advisories/microtar-stack-based-buffer-overflow-via-raw-to-header
https://nvd.nist.gov/vuln/detail/CVE-2026-10293	8,8	UTT HiPER 1200GW	Improper Restriction of Operations within the Bounds of a Memory Buffer	up to 2.5.3-170306	https://github.com/yuezhaoshanmu/cve/blob/main/2.md VulDB https://vuldb.com/cve/CVE-2026-10293 VulDB https://vuldb.com/submit/826416 VulDB https://vuldb.com/vuln/367586 VulDB https://vuldb.com/vuln/367586/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-1784	8,8	The Route OpenShift	External Control of System or Configuration Setting		https://access.redhat.com/security/cve/CVE-2026-1784 Red Hat, Inc. https://bugzilla.redhat.com/show_bug.cgi?id=2436075
https://nvd.nist.gov/vuln/detail/CVE-2026-9330	8,5	IBM WebSphere Application Server	Deserialization of Untrusted Data	9.0, and 8.5	https://www.ibm.com/support/pages/node/7274733
https://nvd.nist.gov/vuln/d	8,2	F5-TTS	Improper Limitation of a Pathname to a	through version 1.1.20	https://github.com/SWivid/F5-TTS/commit/2f53ded68e5f69e248ceb200a51ef4d1dc647936 VulnCheck

etail/CVE-2026-43624			Restricted Directory ('Path Traversal')		https://github.com/SWivid/F5-TTS/issues/1293 VulnCheck https://github.com/SWivid/F5-TTS/pull/1294 VulnCheck https://www.vulncheck.com/advisories/f5-tts-path-traversal-via-finetune-gradio-py-create-data-project
https://nvd.nist.gov/vuln/detail/CVE-2018-25433	8,2	Joomla Component JE Photo Gallery	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.1	http://joomlaextensions.co.in/download/1387375463_JE%20PhotoGallery%20(%20J-%203.0%20).zip VulnCheck https://joomlaextensions.co.in VulnCheck https://www.exploit-db.com/exploits/45930 VulnCheck https://www.vulncheck.com/advisories/joomla-je-photo-gallery-sql-injection-via-categoryid
https://nvd.nist.gov/vuln/detail/CVE-2018-25434	8,2	WP AutoSuggest	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	0.24	https://kaimi.io VulnCheck https://wordpress.org/plugins/wp-autosuggest/ VulnCheck https://www.exploit-db.com/exploits/45977 VulnCheck https://www.vulncheck.com/advisories/wp-autosuggest-sql-injection-via-autosuggest-php
https://nvd.nist.gov/vuln/detail/CVE-2026-49121	8,1	AI Tensor Engine for ROCm (AITER)	Deserialization of Untrusted Data	through 0.1.14	https://github.com/ROCm/aiter/issues/3076 VulnCheck https://github.com/ROCm/aiter/pull/3170 VulnCheck https://www.vulncheck.com/advisories/ai-tensor-engine-for-rocm-aiter-unauthenticated-rce-via-messagequeue-recv-pickle-deserialization
https://nvd.nist.gov/vuln/detail/CVE-2026-47294	8,0	Microsoft Office SharePoint	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47294
https://nvd.nist.gov/vuln/detail/CVE-2026-46243	7,8	Linux kernel	Improper Input Validation		http://www.openwall.com/lists/oss-security/2026/06/01/6
https://nvd.nist.gov/vuln/d	7,8	In addWindow of WindowManagerService.java	Improper Restriction of Rendered UI Layers or Frames		https://source.android.com/docs/security/bulletin/2026/2026-06-01

etail/CVE-2026-28577					
https://nvd.nist.gov/vuln/detail/CVE-2026-24782	7,6	Kiteworks	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Prior to version 9.3.0	https://github.com/kiteworks/security-advisories/security/advisories/GHSA-849r-gm3r-4v5c
https://nvd.nist.gov/vuln/detail/CVE-2026-10290	7,3	Hotel and Tourism Reservation System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/
https://nvd.nist.gov/vuln/detail/CVE-2026-10281	7,3	Enderfga claw-orchestrator	Improper Authentication	up to 3.5.5	https://github.com/Enderfga/claw-orchestrator/
https://nvd.nist.gov/vuln/detail/CVE-2026-10280	7,3	horizon921 mcpilot	Server-Side Request Forgery (SSRF)	0.1.0	https://github.com/horizon921/mcpilot/ VulDB https://github.com/horizon921/mcpilot/issues/1 VulDB https://vuldb.com/cve/CVE-2026-10280 VulDB https://vuldb.com/submit/825426 VulDB https://vuldb.com/vuln/367573 VulDB https://vuldb.com/vuln/367573/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-10287	7,3	SourceCodester SEO Meta Tag Extractor	Server-Side Request Forgery (SSRF)	1.0	https://hackmd.io/@Kq4PsjnpQ5WfoMt8ho48LA/By9GXDkyGe VulDB https://vuldb.com/cve/CVE-2026-10287 VulDB https://vuldb.com/submit/825641 VulDB https://vuldb.com/vuln/367580 VulDB https://vuldb.com/vuln/367580/cti VulDB https://www.sourcecodester.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-45722	7,1	Nextcloud	Improper Neutralization of Special Elements used in an	0.9.0 to before 0.9.7, and 1.0.0 to before 1.0.2	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-5h2w-c7px-hp4j GitHub, Inc. https://github.com/nextcloud/tables/pull/2186 GitHub, Inc. https://hackerone.com/reports/3446689

			SQL Command ('SQL Injection')		
https://nvd.nist.gov/vuln/detail/CVE-2026-49134	7,1	CodexBar	Insecure Temporary File	prior to 0.32.0	https://github.com/steipete/CodexBar/commit/dbc944d46cd4cf7877d1ca47c44556fe573b46e8 VulnCheck https://github.com/steipete/CodexBar/pull/1222 VulnCheck https://github.com/steipete/CodexBar/releases/tag/v0.32.0 VulnCheck https://www.vulncheck.com/advisories/codexbar-privilege-escalation-via-cli-installer-temp-file

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-2024-21182 Oracle WebLogic Server Unspecified Vulnerability**	**https://www.cisa.gov/news-events/alerts/2026/06/01/cisa-adds-one-known-exploited-vulnerability-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
Anthropic to Open Mythos AI to EU's ENISA	https://www.darkreading.com/cyber-risk/anthropic-mythos-ai-eu-enisa
Infosecurity Europe: OWASP Forms New Agentic Research Council	https://www.infosecurity-magazine.com/news/owasp-new-agentic-research-council/
Iran-Linked Hackers Destroy IT, Backups, and Recovery Systems in Cyberattack targeting Middle East	https://cybersecuritynews.com/iran-linked-hackers-destroy-it-backups-and-recovery-systems/
Microsoft Tightens Entra ID Password Resets With New Authentication Change	https://cybersecuritynews.com/microsoft-tightens-entra-id-password-resets/

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 Red Hat Cloud Services npm Packages Compromised to Deploy Credential-Stealing Malware	https://cybersecuritynews.com/red-hat-cloud-services-npm-packages/

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
PAN-OS GlobalProtect Authentication Bypass (CVE-2026-0257) Under Active Exploitation	https://thehackernews.com/2026/05/pan-os-globalprotect-authentication.html
Critical WP Maps Pro Flaw Actively Exploited to Create Admin Accounts	https://thehackernews.com/2026/06/critical-wp-maps-pro-flaw-actively.html
Weekly Recap: New Linux Flaw, PAN-OS Exploit, AI-Powered Attacks, OAuth Phishing and More	https://thehackernews.com/2026/06/weekly-recap-new-linux-flaw-pan-os.html
Critical Windows Netlogon Vulnerability in Attackers' Crosshairs	https://www.securityweek.com/critical-windows-netlogon-vulnerability-in-attackers-crosshairs/
19-Year-Old Linux Kernel Vulnerability Exposes Systems to Root Access	https://www.securityweek.com/19-year-old-linux-kernel-vulnerability-exposes-systems-to-root-access/
Recent Palo Alto Networks Vulnerability Exploited for Weeks	https://www.securityweek.com/recent-palo-alto-networks-vulnerability-exploited-for-weeks/
Exploit Code Published for Critical Flowise RCE Vulnerability	https://www.securityweek.com/category/vulnerabilities/
Microsoft's Zero-Day Legal Threats Spark Backlash	https://www.darkreading.com/application-security/microsoft-zero-day-legal-threats-backlash
Critical Flowise Flaw Gives Attackers Full Server Control	https://www.infosecurity-magazine.com/news/flowise-mcp-rce-poc/
New CIFSwitch Linux flaw gives root on multiple distributions	https://www.bleepingcomputer.com/news/security/new-cifswitch-linux-flaw-gives-root-on-multiple-distributions/
Critical WP Maps Pro Vulnerability Allow Attackers to Create Administrator Account	https://cybersecuritynews.com/wp-maps-pro-vulnerability/
IBM WebSphere Server Vulnerable to Remote Code Execution Attack Via Crafted Request	https://cybersecuritynews.com/ibm-websphere-server-remote-code-execution/
Critical Magento Cache Plugin Vulnerability Enables Remote Code Execution Attacks	https://cybersecuritynews.com/magento-cache-plugin-vulnerability/
Critical MCP Toolbox Vulnerability Impacts Enterprise Database onnectors	https://cybersecuritynews.com/mcp-toolbox-vulnerability/
Critical Plesk Vulnerability Let Users Execute Arbitrary Commands on the Server	https://cybersecuritynews.com/plesk-command-execution-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
GitLab Patches Multiple Duo AI, DoS, and Authorization Flaws in Community and Enterprise Edition	https://cybersecuritynews.com/gitlab-patches-duo-ai-dos-flaws/

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
Attackers Abuse Shared Content for ChatGPT Phishing Campaign	https://www.infosecurity-magazine.com/news/attackers-shared-content-chatgpt/
FSB Group Gamaredon Hides Worm in Windows Data Streams	https://www.infosecurity-magazine.com/news/gamaredon-worm-ntfs-data-streams/
WP Maps Pro bug exploited to create admin accounts on WordPress sites	https://www.bleepingcomputer.com/news/security/wp-maps-pro-bug-exploited-to-create-admin-accounts-on-wordpress-sites/
Gamaredon APT Hides Malware in Windows Features and Abuses Cloud Platforms for C2	https://cybersecuritynews.com/gamaredon-apt-hides-malware-in-windows-c2/
Hackers Use Meta's AI Bot to Reset Passwords and Hijack Instagram Accounts	https://cybersecuritynews.com/metas-ai-support-bot-instagram/
Android Banking Trojan OverlayPhantom Abuses Accessibility Service to Control Devices	https://cybersecuritynews.com/android-banking-trojan-overlayphantom/
Attackers Abuse Docker and Kubernetes Misconfigurations to Compromise Host Systems	https://cybersecuritynews.com/attackers-abuse-docker-and-kubernetes-misconfigurations/
SmartApeSG Campaign Uses ClickFix Scripts to Infect Windows Hosts With RAT Malware	https://cybersecuritynews.com/smartapesg-campaign-uses-clickfix-scripts/
Iranian Hackers Abuse AppDomainManager Hijacking to Evade EDR Detection	https://cybersecuritynews.com/iranian-hackers-abuse-appdomainmanager-hijacking/
SideCopy Hackers Deploy Persistent XenoRAT Malware to Target Afghanistan Finance Ministry	https://cybersecuritynews.com/sidecopy-hackers-deploy-persistent-xenorat-malware/
Hackers Attacking Signal Users to Steal Backups in New Wave of Attacks	https://cybersecuritynews.com/hackers-attacking-signal-users/
GREYVIBE Hackers Leverage ChatGPT and Google Gemini to Fuel Cyberattacks	https://cybersecuritynews.com/greyvibe-hackers-chatgpt-and-google-gemini/

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/
The CISO Executive Toolkit (Free Download)	https://thehackernews.uk/wiz-ciso-bundle
Secure Coding Best Practices: Practical Guide + Cheat Sheet for Developers	https://thehackernews.uk/secure-coding-wiz-cheat
Top 10 Best Malware Sandbox Tools for Security Teams in 2026	https://cybersecuritynews.com/best-malware-sandbox-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/