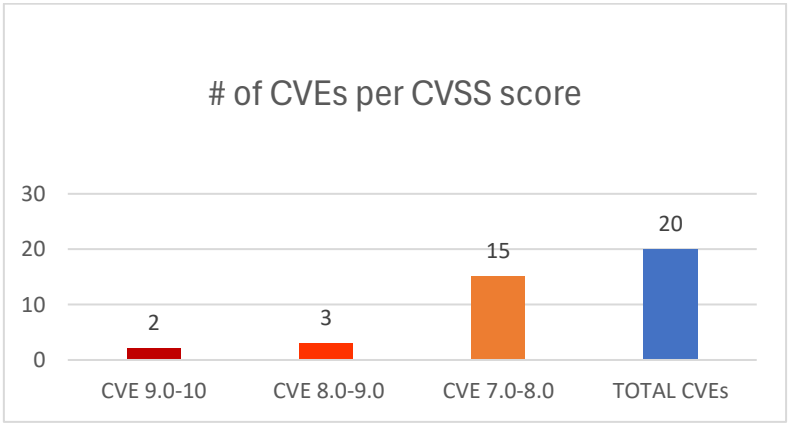
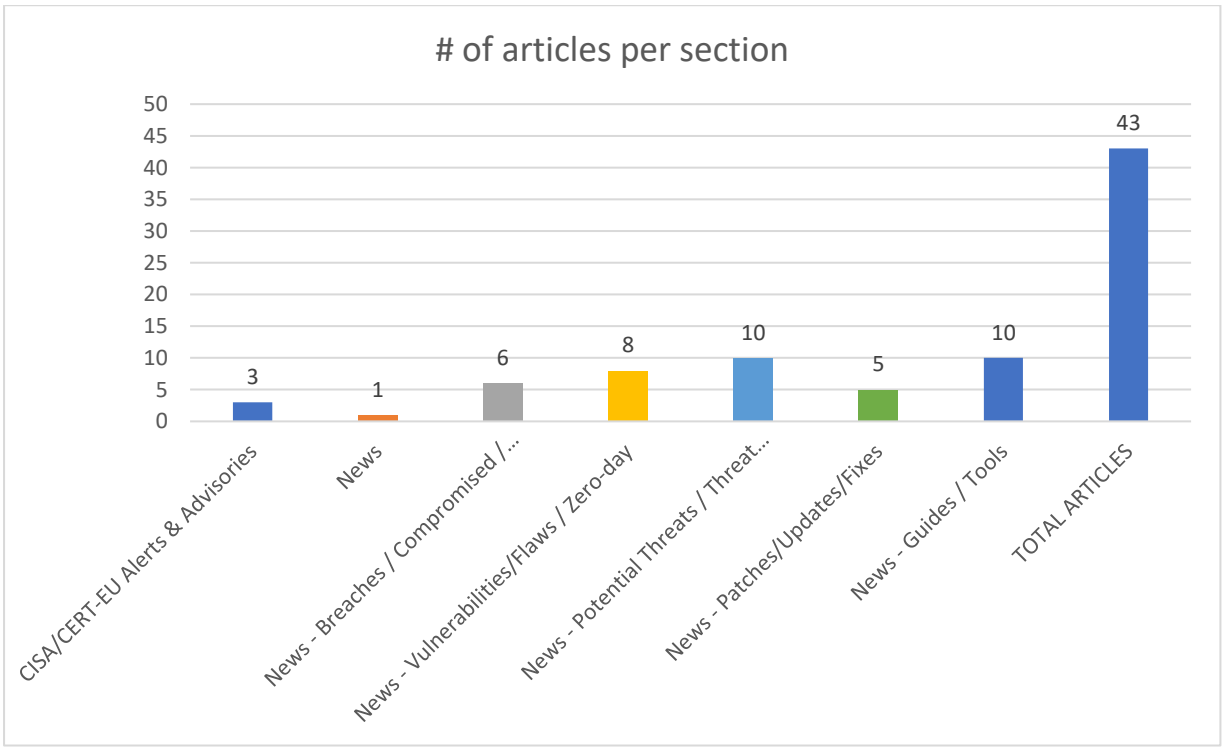
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 25/03/2026 - 27/03/2026





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-2026-32536	9,9	Green Downloads halfdata-paypal-green-downloads	Unrestricted Upload of File with Dangerous Type	from n/a through <= 2.08	https://patchstack.com/database/Wordpress/Plugin/halfdata-paypal-green-downloads/vulnerability/wordpress-green-downloads-plugin-2-08-arbitrary-file-upload-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-32573	9,1	Nelio Software Nelio AB Testing nelio-ab-testing	Improper Control of Generation of Code ('Code Injection')	from n/a through <= 8.2.7	https://patchstack.com/database/Wordpress/Plugin/nelio-ab-testing/vulnerability/wordpress-nelio-ab-testing-plugin-8-2-7-remote-code-execution-rce-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-4840	8,8	Netcore Power 15AX	Improper Neutralization of Special Elements used in a Command ('Command Injection')	up to 3.0.0.6938	https://github.com/fakervsbln/netcore-power15ax-cve VulDB https://vuldb.com/?ctiid.353146 VulDB https://vuldb.com/?id.353146 VulDB https://vuldb.com/?submit.776127
https://nvd.nist.gov/vuln/detail/CVE-2026-32534	8,5	JoomSky JS Help Desk js-support-ticket	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	from n/a through <= 3.0.3	https://patchstack.com/database/Wordpress/Plugin/js-support-ticket/vulnerability/wordpress-js-help-desk-plugin-3-0-3-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-32531	8,1	gavias Kunco	Improper Control of Filename for Include/Require Statement in	from n/a through < 1.4.5	https://patchstack.com/database/Wordpress/Theme/kunco/vulnerability/wordpress-kunco-theme-1-4-5-local-file-inclusion-vulnerability?_s_id=cve

			PHP Program ('PHP Remote File Inclusion)		
https://nvd.nist.gov/vuln/detail/CVE-2026-32680	7,8	RATOC RAID Monitoring Manager for Windows	Incorrect Default Permissions		https://jvn.jp/en/jp/JVN08057419/ JPCERT/CC https://www.ratocsystems.com/topics/userinfo/raidmanager202508/
https://nvd.nist.gov/vuln/detail/CVE-2026-33932	7,6	OpenEMR	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Prior to version 8.0.0.3	https://github.com/openemr/openemr/commit/95e6078889b5399b12b59117f998560cd94bd47d GitHub, Inc. https://github.com/openemr/openemr/releases/tag/v8_0_0_3 GitHub, Inc. https://github.com/openemr/openemr/security/advisories/GHSA-g77x-9p3x-2j8f
https://nvd.nist.gov/vuln/detail/CVE-2026-33287	7,5	LiquidJS	Improper Input Validation	Prior to version 10.25.1	https://github.com/harttle/liquidjs/commit/35d523026345d80458df24c72e653db78b5d061d GitHub, Inc. https://github.com/harttle/liquidjs/security/advisories/GHSA-6q5m-63h6-5x4v
https://nvd.nist.gov/vuln/detail/CVE-2026-32546	7,5	StellarWP	Missing Authorization	from n/a through <= 3.2.22	https://patchstack.com/database/Wordpress/Plugin/restrict-content/vulnerability/wordpress-restrict-content-plugin-3-2-22-broken-access-control-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-32537	7,5	nK Visual Portfolio, Photo Gallery & Post Grid visual-portfolio	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion)	from n/a through <= 3.5.1	https://patchstack.com/database/Wordpress/Plugin/visual-portfolio/vulnerability/wordpress-visual-portfolio-photo-gallery-post-grid-plugin-3-5-1-local-file-inclusion-vulnerability?_s_id=cve

https://nvd.nist.gov/vuln/detail/CVE-2026-32538	7,5	Noor Alam SMTP Mailer smtp-mailer	Insertion of Sensitive Information Into Sent Data	from n/a through <= 1.1.24	https://patchstack.com/database/Wordpress/Plugin/smtp-mailer/vulnerability/wordpress-smtp-mailer-plugin-1-1-24-sensitive-data-exposure-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-33247	7,4	NATS-Server	Insertion of Sensitive Information Into Debugging Code	Prior to versions 2.11.15 and 2.12.6	https://advisories.nats.io/CVE/secnote-2026-14.txt GitHub, Inc. https://github.com/nats-io/nats-server/security/advisories/GHSA-x6g4-f6q3-fqvv
https://nvd.nist.gov/vuln/detail/CVE-2026-4844	7,3	Online Food Ordering System	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	1.0	https://code-projects.org/ VulDB https://gist.github.com/HxH404/8e5bd42c0f968a92a23edc5e7b879955 VulDB https://vuldb.com/?ctiid.353149 VulDB https://vuldb.com/?id.353149 VulDB https://vuldb.com/?submit.776137
https://nvd.nist.gov/vuln/detail/CVE-2026-4842	7,3	Online Enrollment System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/dsdsadawada/CVE1/issues/4 VulDB https://itsourcecode.com/ VulDB https://vuldb.com/?ctiid.353148 VulDB https://vuldb.com/?id.353148 VulDB https://vuldb.com/?submit.776132
https://nvd.nist.gov/vuln/detail/CVE-2026-4838	7,3	SourceCodester Malawi Online Market	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	1.0	https://github.com/WHOAMI-xiaoyu/CVE/blob/main/CVE_8.md VulDB https://vuldb.com/?ctiid.353141 VulDB https://vuldb.com/?id.353141 VulDB https://vuldb.com/?submit.776081 VulDB https://www.sourcecodester.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-4784	7,3	Simple Laundry System	Improper Neutralization of Special Elements in Output Used by a Downstream	1.0	https://code-projects.org/ VulDB https://github.com/zzb1388/cve2/issues/1 VulDB https://vuldb.com/?ctiid.352801 VulDB https://vuldb.com/?id.352801 VulDB https://vuldb.com/?submit.775811

			Component ('Injection')		
https://nvd.nist.gov/vuln/detail/CVE-2026-3328	7,2	The Frontend Admin by DynamiApps plugin for WordPress	Deserialization of Untrusted Data	up to, and including, 3.28.31	https://plugins.trac.wordpress.org/browser/acf-frontend-form-element/tags/3.28.27/main/admin/admin-pages/forms/settings.php#L419 Wordfence https://plugins.trac.wordpress.org/browser/acf-frontend-form-element/trunk/main/admin/admin-pages/forms/settings.php#L419 Wordfence https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3486785%40acf-frontend-form-element&new=3486785%40acf-frontend-form-element&sfp_email=&sfph_mail= Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/0faa8f07-88c1-4638-9de5-e202807866e1?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-32532	7,1	ThemeHunk Contact Form & Lead Form Elementor Builder	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through <= 2.0.1	https://patchstack.com/database/Wordpress/Plugin/lead-form-builder/vulnerability/wordpress-contact-form-lead-form-elementor-builder-plugin-2-0-1-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-32526	7,1	VillaTheme Abandoned Cart Recovery for WooCommerce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from n/a through <= 1.1.10	https://patchstack.com/database/Wordpress/Plugin/woo-abandoned-cart-recovery/vulnerability/wordpress-abandoned-cart-recovery-for-woocommerce-plugin-1-1-10-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-4824	7,0	Enter Software Iperius Backup	Incorrect Privilege Assignment	up to 8.7.3	https://github.com/0truust/iperius-backup-security-advisories/blob/main/advisories/privilege-escalation-rce.md VulDB https://vuldb.com/?ctiid.353124 VulDB https://vuldb.com/?id.353124 VulDB

				https://vuldb.com/?submit.774220 VulDB https://www.iperiusbackup.com/download-software-backup.aspx

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-2026-33017 Langflow Code Injection Vulnerability**	**https://www.cisa.gov/news-events/alerts/2026/03/25/cisa-adds-one-known-exploited-vulnerability-catalog**
CISA Adds One Known Exploited Vulnerability to Catalog	▪ **CVE-2025-53521 F5 BIG-IP Remote Code Execution Vulnerability**	**https://www.cisa.gov/news-events/alerts/2026/03/27/cisa-adds-one-known-exploited-vulnerability-catalog**
CISA Adds One Known Exploited Vulnerability to Catalog	▪ **CVE-2026-33634 Aqua Security Trivy Embedded Malicious Code Vulnerability**	**https://www.cisa.gov/news-events/alerts/2026/03/26/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
Addressing the Supply Chain Risk: Why Protecting Smaller Companies is the Key to Keeping Big Enterprises Secure	https://www.darkreading.com/vulnerabilities-threats/addressing-the-supply-chain-risk-why-protecting-smaller-companies-is-the-key-to-keeping-big-enterprises-secure

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
WebRTC Skimmer Bypasses CSP to Steal Payment Data from E-Commerce Sites	https://thehackernews.com/2026/03/webrtc-skimmer-bypasses-csp-to-steal.html
China-Linked Hackers Breach Southeast Asian Military Systems in Long-Running Spy Campaign	https://cybersecuritynews.com/china-linked-hackers-breach-southeast-asian-military-systems/
Open Directory Malware Campaign Uses Obfuscated VBS, PNG Loaders and RAT Payloads	https://cybersecuritynews.com/open-directory-malware-campaign/
LiteLLM PyPI Package With 95 Million Downloads Compromised by TeamPCP Hackers	https://cybersecuritynews.com/litellm-package-compromised/
Aqua Security's Trivy Scanner Compromised in Supply Chain Attack	https://cybersecuritynews.com/trivy-scanner-compromised/
Telnyx PyPI Package With 742,000 downloads Compromised in TeamPCP Supply Chain Attack	https://cybersecuritynews.com/telnyx-pypi-package-compromised/

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
TP-Link warns users to patch critical router auth bypass flaw	https://www.bleepingcomputer.com/news/security/tp-link-warns-users-to-patch-critical-router-auth-bypass-flaw/
Citrix urges admins to patch NetScaler flaws as soon as possible	https://www.bleepingcomputer.com/news/security/citrix-urges-admins-to-patch-netscaler-flaws-as-soon-as-possible/
F5 NGINX Plus and Open Source Vulnerability Allow Attackers to Execute Code Using MP4 file	https://cybersecuritynews.com/f5-nginx-plus-and-open-source-vulnerability/
Multiple TP-Link Vulnerabilities Allow Attackers to Execute Arbitrary Commands on System	https://cybersecuritynews.com/multiple-tp-link-vulnerabilities/
ClawHub Vulnerability Let Attackers Manipulate Rankings to Become the #1 Skill	https://cybersecuritynews.com/clawhub-vulnerability-manipulate-rankings-to-become-the-1-skill/
Red Hat Warns of Malware Code Embedded in Popular Linux Tool Allow Unauthorized Access to Systems	https://cybersecuritynews.com/linux-tool-malware-embedded/
New Windows Error Reporting Vulnerability Lets Attackers Escalate to Gain SYSTEM Access	https://cybersecuritynews.com/new-windows-error-reporting-vulnerability/
Critical NVIDIA Vulnerabilities Enables RCE and DoS Attacks	https://cybersecuritynews.com/nvidia-vulnerabilities-rce-attacks/

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
iOS, macOS 26.4 Roll Out With Fresh Security Patches	https://www.securityweek.com/ios-macos-26-4-roll-out-with-fresh-security-updates/
Firefox 149.0 Released With Free Built-in VPN With 50 GB Monthly Data Limit	https://cybersecuritynews.com/firefox-149-0-built-in-vpn/
Node.js Patches Multiple Vulnerabilities That Enable DoS Attacks and Process Crashes	https://cybersecuritynews.com/node-js-patches-multiple-vulnerabilities/
Firefox 149 Released With Patch for 37 Vulnerabilities that Enables Remote Attacks	https://cybersecuritynews.com/firefox-149-released/
Kali Linux 2026.1 Released With 8 New Hacking Tools	https://cybersecuritynews.com/kali-linux-2026-1/

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
Fake VS Code Security Alerts on GitHub Used to Push Malware in Widespread Phishing Campaign	https://cybersecuritynews.com/fake-npm-install-messages-hide-rat-malware/
Ghost SPN Attack Lets Hackers Conduct Stealthy Kerberoasting Under the Radar	https://cybersecuritynews.com/ghost-spn-attack/
Mirai-Based Botnets Evolve Into Massive DDoS and Proxy Abuse Threat	https://cybersecuritynews.com/mirai-based-botnets-evolve-into-massive-ddos/
Linux Ransomware Pay2Key Attacking Servers, Virtualization Platforms, and Cloud Environments	https://cybersecuritynews.com/linux-ransomware-pay2key-attacking-organizations-ervers/
SmartApeSG ClickFix Campaign Delivers Remcos, NetSupport RAT, StealC and Sectop RAT	https://cybersecuritynews.com/smartapesg-clickfix-campaign-delivers-remcos/
AI-Assisted 'OpenClaw Trap' Campaign Uses Trojanized GitHub Repos to Target Developers and Gamers	https://cybersecuritynews.com/ai-assisted-openclaw-trap-campaign-uses-trojanized-github-repos/
Five Malicious npm Packages Target Crypto Developers, Exfiltrate Wallet Keys via Telegram	https://cybersecuritynews.com/five-malicious-npm-packages/
Google Authenticator's Hidden Passkey Architecture Could Open New Passwordless Attack Paths	https://cybersecuritynews.com/google-authenticators-hidden-passkey-architecture/
Hackers Use Phishing ZIP Files to Deploy PXA Stealer Against Financial Firms	https://cybersecuritynews.com/hackers-use-phishing-zip-files/
Open VSX Bug Let Malicious VS Code Extensions Bypass Pre-Publish Security Checks	https://thehackernews.com/2026/03/open-vsx-bug-let-malicious-vs-code.html

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

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/