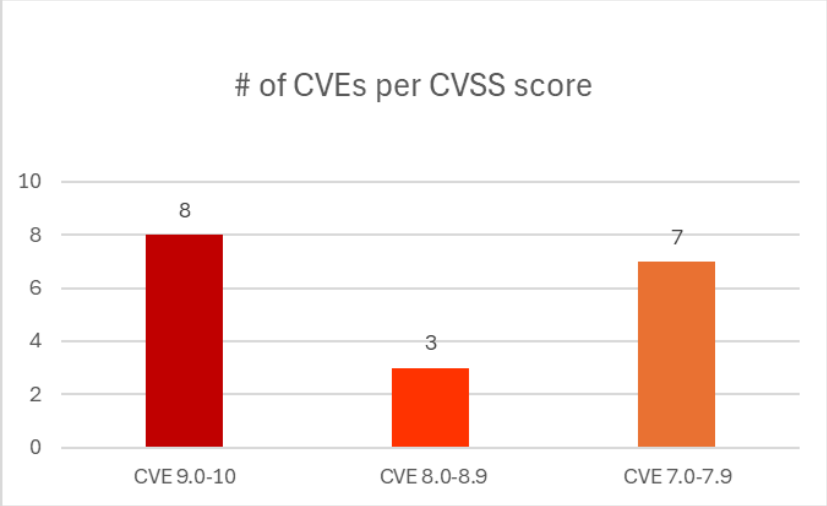
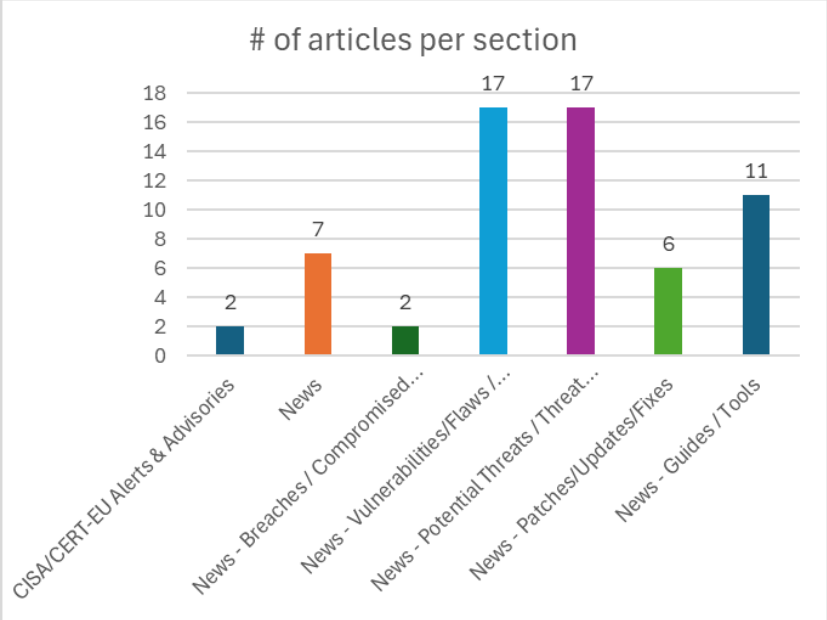
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 15/04/2026 - 17/04/2026





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-2026-20147	9,9	Cisco	Improper Neutralization of Special Elements used in a Command ('Command Injection')		https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-traversal-8bYndVrZ
https://nvd.nist.gov/vuln/detail/CVE-2026-20180	9,9	Cisco	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')		https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-4fverepv
https://nvd.nist.gov/vuln/detail/CVE-2026-20186	9,9	Cisco	Improper Neutralization of Special Elements used in a Command ('Command Injection')		https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-4fverepv
https://nvd.nist.gov/vuln/detail/CVE-2026-20184	9,8	Cisco	Improper Certificate Validation		https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-cui-cert-8jSZYhWL
https://nvd.nist.gov/vuln/detail/CVE-2026-40504	9,8	Creolabs Gravity	Heap-based Buffer Overflow	before 0.9.6	https://github.com/marcobambini/gravity/commit/18b9195598d9b944376754c6d1ad76e38a4adca1 VulnCheck https://github.com/marcobambini/gravity/issues/437 VulnCheck https://github.com/marcobambini/gravity/releases/tag/0.9.6 VulnCheck https://www.vulncheck.com/advisories/creolabs-gravity-heap-buffer-overflow-via-gravity-vm-exec
https://nvd.nist.gov/vuln/detail/CVE-2026-4880	9,8	The Barcode Scanner (+Mobile App) – Inventory manager, Order fulfillment system, POS (Point of Sale) plugin for WordPress	Improper Privilege Management	up to, and including, 1.11.0	https://plugins.trac.wordpress.org/browser/barcode-scanner-lite-pos-to-manage-products-inventory-and-orders/trunk/src/Core.php?rev=3391688#L498 Wordfence https://plugins.trac.wordpress.org/changeset/3506824/barcode-scanner-lite-pos-to-manage-products-inventory-and-orders#file30 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/a213e844-a0d3-4123-9f72-caef7702804c?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-6296	9,6	Google Chrome	Heap-based Buffer Overflow	Heap buffer overflow in ANGLE in Google Chrome prior to 147.0.7727.101	https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_15.html https://issues.chromium.org/issues/490170083

https://nvd.nist.gov/vuln/detail/CVE-2026-6388	9,1	ArgoCD Image Updater	Insufficient Granularity of Access Control		https://access.redhat.com/security/cve/CVE-2026-6388 Red Hat, Inc. https://bugzilla.redhat.com/show_bug.cgi?id=2458766
https://nvd.nist.gov/vuln/detail/CVE-2026-6363	8,8	V8 in Google Chrome	Access of Resource Using Incompatible Type ('Type Confusion')	prior to 147.0.7727.101	https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_15.html Chrome https://issues.chromium.org/issues/495751197
https://nvd.nist.gov/vuln/detail/CVE-2026-40764	8,1	Syed Balkhi Contact Form by WPForms	Cross-Site Request Forgery (CSRF)	from n/a through <= 1.10.0.2	https://patchstack.com/database/Wordpress/Plugin/wpforms-lite/vulnerability/wordpress-contact-form-by-wpforms-plugin-1-10-0-2-cross-site-request-forgery-csrf-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-40960	8,1	Luanti 5	Always-Incorrect Control Flow Implementation	before 5.15.2	https://github.com/luanti-org/luanti/commit/0faf529bc4b89e70a275ed1162047815118f2413 MITRE https://github.com/luanti-org/luanti/commit/827fd4cf7f989482b2dad381fa4afd642ea73e8c MITRE https://github.com/luanti-org/luanti/security/advisories/GHSA-22c4-238c-m5j4
https://nvd.nist.gov/vuln/detail/CVE-2026-40745	7,6	Element Pack Elementor Addons	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')		https://patchstack.com/database/Wordpress/Plugin/bdthemes-element-pack-lite/vulnerability/wordpress-element-pack-elementor-addons-plugin-8-4-2-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-40719	7,5	Deadwood in MaraDNS	Always-Incorrect Control Flow Implementation	3.5.0036	https://github.com/samboy/MaraDNS/security/advisories/GHSA-cfc6-vhrv-62cj CISA-ADP, MITRE https://maradns.samiam.org/changelog.html
https://nvd.nist.gov/vuln/detail/CVE-2026-5050	7,5	The Payment Gateway for Redsys & WooCommerce Lite plugin for WordPress	Improper Verification of Cryptographic Signature	up to, and including, 7.0.0	https://plugins.trac.wordpress.org/changeset/3501998/woo-redsys-gateway-light Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/80544889-8efc-4aa0-a690-774b1ee6a1a0?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-6351	7,5	MailGates/MailAudit developed by Openfind	Improper Neutralization of CRLF Sequences ('CRLF Injection')		https://www.twcert.org.tw/en/cp-139-10843-9ff91-2.html TWCERT/CC https://www.twcert.org.tw/tw/cp-132-10844-1405d-1.html
https://nvd.nist.gov/vuln/detail/CVE-2026-6372	7,5	Accept Cryptocurrencies with Plisio	Missing Authorization	from n/a through 2.0.5	https://patchstack.com/database/wordpress/plugin/plisio-payment-gateway-for-woocommerce/vulnerability/wordpress-accept-cryptocurrencies-with-plisio-plugin-2-0-5-payment-bypass-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-41035	7,4	In rsync	Improper Handling of Length Parameter Inconsistency	3.0.1 through 3.4.1	https://github.com/RsyncProject/rsync/issues/871 https://github.com/RsyncProject/rsync/releases https://www.openwall.com/lists/oss-security/2026/04/16/2
https://nvd.nist.gov/vuln/detail/CVE-2026-23772	7,3	Dell	Improper Privilege Management	Dell Storage Manager - Replay Manager for Microsoft Servers, version(s) 8.0	https://www.dell.com/support/kbdoc/en-us/000453020/dsa-2026-058-security-update-for-dell-storage-manager-replay-manager-for-microsoft-servers-vulnerabilities

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-2009-0238 Microsoft Office Remote Code Execution Vulnerability ▪ CVE-2026-32201 Microsoft SharePoint Server Improper Input Validation Vulnerability	https://www.cisa.gov/news-events/alerts/2026/04/14/cisa-adds-two-known-exploited-vulnerabilities-catalog
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2026-34197 Apache ActiveMQ Improper Input Validation Vulnerability	https://www.cisa.gov/news-events/alerts/2026/04/16/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
MuddyWater-Style Hackers Scan 12,000+ Systems Before Hitting Middle East Critical Sectors	https://cybersecuritynews.com/muddywater-style-hackers-scan-12000-systems/
European Cybersecurity Agency ENISA Seeks Top-Tier Status in CVE Program	https://www.infosecurity-magazine.com/news/enisa-europe-seeks-top-level-root/
AI Companies to Play Bigger Role in CVE Program, Says CISA	https://www.infosecurity-magazine.com/news/ai-companies-to-play-bigger-role/
Prepping for 'Q-Day': Why Quantum Risk Management Should Start Now	https://www.darkreading.com/cyber-risk/preparing-q-day-quantum-risk-management
Microsoft Confirms Windows 11 Updates May Force Users to Enter BitLocker Recovery Key	https://cybersecuritynews.com/windows-11-update-bitlocker/
Microsoft 365 Web Services Hit by Google Chrome 147 Compatibility Issue	https://cybersecuritynews.com/microsoft-365-chrome-147-issue/
Two U.S. Nationals Sentenced for Running Laptop Farm for DPRK Remote Workers	https://cybersecuritynews.com/two-u-s-nationals-sentenced/

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
25,000+ Endpoints Exposed by Dragon Boss Solutions Update Domain Supply Chain Attack	https://cybersecuritynews.com/25000-endpoints-exposed-by-dragon-boss-solutions/
McGraw Hill Confirms Data Breach Exposing 13.5 Million Users' Personal Data	https://cybersecuritynews.com/mcgraw-hill-confirms-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
Splunk Enterprise and Cloud Platform Vulnerability Enables Remote Code Execution Attacks	https://cybersecuritynews.com/splunk-enterprise-and-cloud-platform-vulnerability/
Critical Chrome Vulnerabilities Let Attackers Execute Arbitrary Code – Update Now!	https://cybersecuritynews.com/chrome-vulnerabilities/
Windows Active Directory Vulnerability Allows Attackers to Execute Malicious Code	https://cybersecuritynews.com/windows-active-directory-vulnerability/
New PHP Composer Vulnerability Let Attackers Execute Arbitrary Commands	https://cybersecuritynews.com/php-composer-vulnerability/
Adobe Acrobat Reader Vulnerabilities Let Attackers Execute Arbitrary Code	https://cybersecuritynews.com/adobe-acrobat-reader-vulnerabilities-patch/
Hackers Hide Backdoor in Trusted WordPress Plugins for 8 Months Before Activating Malware	https://cybersecuritynews.com/hackers-hide-backdoor-in-trusted-wordpress-plugins/
OpenAI Launches GPT-5.4 with Reverse Engineering, Vulnerability and Malware Analysis Features	https://cybersecuritynews.com/openai-launches-gpt-5-4/
Microsoft SharePoint Server 0-Day Vulnerability Actively Exploited in Attacks	https://cybersecuritynews.com/sharepoint-server-0-day-vulnerability/
Critical Nginx-ui MCP Flaw Actively Exploited in the Wild	https://www.infosecurity-magazine.com/news/nginx-ui-mcp-flaw-actively/
Actively Exploited nginx-ui Flaw (CVE-2026-33032) Enables Full Nginx Server Takeover	https://thehackernews.com/2026/04/critical-nginx-ui-vulnerability-cve.html
CISA flags Windows Task Host vulnerability as exploited in attacks	https://www.bleepingcomputer.com/news/security/cisa-flags-windows-task-host-vulnerability-as-exploited-in-attacks/
Microsoft Defender 0-Day Vulnerability "RedSun" Enables Full SYSTEM Access	https://cybersecuritynews.com/defender-0-day-redsun/
EU's New Age Verification App Can Be Hacked Within 2 Minutes, Researchers Claim	https://cybersecuritynews.com/eus-age-verification-app/
SpankRAT Exploits Windows Explorer Processes for Stealth and Delayed Detection	https://cybersecuritynews.com/spankrat-exploits-windows-process/
Critical Cisco ISE Vulnerabilities Let Remote Attackers Execute Malicious Code	https://cybersecuritynews.com/cisco-ise-vulnerabilities/

Cisco Webex Services Vulnerability Let Remote Attacker Impersonate Any User	https://cybersecuritynews.com/cisco-webex-services-vulnerability/
Nginx-ui Vulnerability Actively Exploited in Attack – Enables Full Server Takeover	https://cybersecuritynews.com/nginx-ui-vulnerability-exploited/

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
Microsoft Releases Cumulative Update KB5083769 for Windows 11, Version 25H2 and 24H2	https://cybersecuritynews.com/microsoft-cumulative-update-windows-11/
Microsoft Fixes Two Zero-Days in April Patch Tuesday	https://www.infosecurity-magazine.com/news/microsoft-two-zerodays-april-patch/
Microsoft Issues Patches for SharePoint Zero-Day and 168 Other New Vulnerabilities	https://thehackernews.com/2026/04/microsoft-issues-patches-for-sharepoint.html
April Patch Tuesday Fixes Critical Flaws Across SAP, Adobe, Microsoft, Fortinet, and More	https://thehackernews.com/2026/04/april-patch-tuesday-fixes-critical.html
Fortinet Patches Critical FortiSandbox Vulnerabilities	https://www.securityweek.com/fortinet-patches-critical-fortisandbox-vulnerabilities/
Two Vulnerabilities Patched in Ivanti Neurons for ITSM	https://www.securityweek.com/two-vulnerabilities-patched-in-ivanti-neurons-for-itsm/

Potential threats / Threat intelligence

Η συγκεκριμένη ενότητα ασχολείται με νέες απειλές, εξελιγμένα malware και τεχνικές επιθέσεων που έχουν εντοπιστεί σε πραγματικές συν-θήκες. Περι-λαμβάνονται αναφορές σε εργαλεία που χρησιμοποιούν οι επιτιθέμενοι, αλλά και δείκτες (IoCs) που μπορούν να χρησιμοποιηθούν στην άμυνα.

Σύντομη περιγραφή / Τίτλος	URL
Fake Adobe Reader Download Delivers ScreenConnect Through Stealthy In-Memory Loader	https://cybersecuritynews.com/fake-adobe-reader-download-delivers-screenconnect/
1,250+ C2 Servers Mapped Across Russian Hosting Across 165 Providers	https://cybersecuritynews.com/1250-c2-servers-mapped-across-russian-hosting/
Hackers Abuse Google Discover With AI-Generated Content to Push Malicious Notifications	https://cybersecuritynews.com/hackers-abuse-google-discover-with-ai-generated-content/
Hackers Using Google Cloud Storage to Bypass Email Filters and Deliver Remcos RAT	https://cybersecuritynews.com/hackers-using-google-cloud-storage-to-bypass-email-filters/
Hackers Create Hidden Mailbox Rules in Microsoft 365 to Intercept Sensitive Business Emails	https://cybersecuritynews.com/hackers-create-hidden-mailbox-rules-in-microsoft-365/
Agentic LLM Browsers Expose New Attack Surface for Prompt Injection and Data Theft	https://cybersecuritynews.com/agentic-llm-browsers-expose-new-attack-surface/
FUNNULL-Linked Triad Nexus Resurfaces With 175+ Rotating CNAME Domains and Global Scam Portals	https://cybersecuritynews.com/funnull-linked-triad-nexus-resurfaces/
Windows BitLocker Vulnerability Allows Attacker to Bypass Security Feature	https://cybersecuritynews.com/windows-bitlocker-security-vulnerability/
New JanaWare Ransomware Targets Turkish Users Through Customized Adwind RAT	https://cybersecuritynews.com/new-janaware-ransomware-targets-turkish-users/
Microsoft Defender 0-Day Vulnerability Enables Privilege Escalation Attack	https://cybersecuritynews.com/microsoft-defender-0-day-vulnerability/
6-Year Ransomware Campaign Targets Turkish Homes & SMBs	https://www.darkreading.com/cyberattacks-data-breaches/6-year-ransomware-campaign-turkish-homes-smbs
Hackers Target Trucking and Freight Firms to Steal Real-World Cargo Shipments	https://cybersecuritynews.com/hackers-target-trucking-and-freight-firms/
New UAC-0247 Campaign Steals Browser and WhatsApp Data From Hospitals and Governments	https://cybersecuritynews.com/new-uac-0247-campaign-steals-browser-and-whatsapp-data/
Fake Proton VPN Sites and Gaming Mods Spread NWHStealer in New Windows Malware Campaign	https://cybersecuritynews.com/fake-proton-vpn-sites-and-gaming-mods/
Hackers Abuse n8n AI Workflow Automation to Deliver Malware Through Trusted Webhooks	https://cybersecuritynews.com/hackers-abuse-n8n-ai-workflow-automation/
31 High-Impact Vulnerabilities Exploited in March as Interlock Hits Cisco FMC Zero-Day	https://cybersecuritynews.com/vulnerabilities-exploited-as-interlock-hits-cisco-fmc/
New Chrome Privacy Analysis Shows How Fingerprinting and Header Leaks Can Expose Users	https://cybersecuritynews.com/new-chrome-privacy-analysis/

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

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/