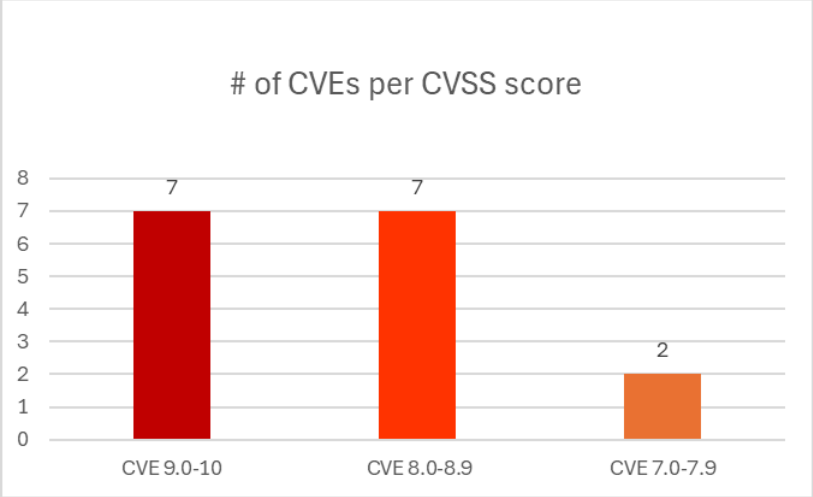
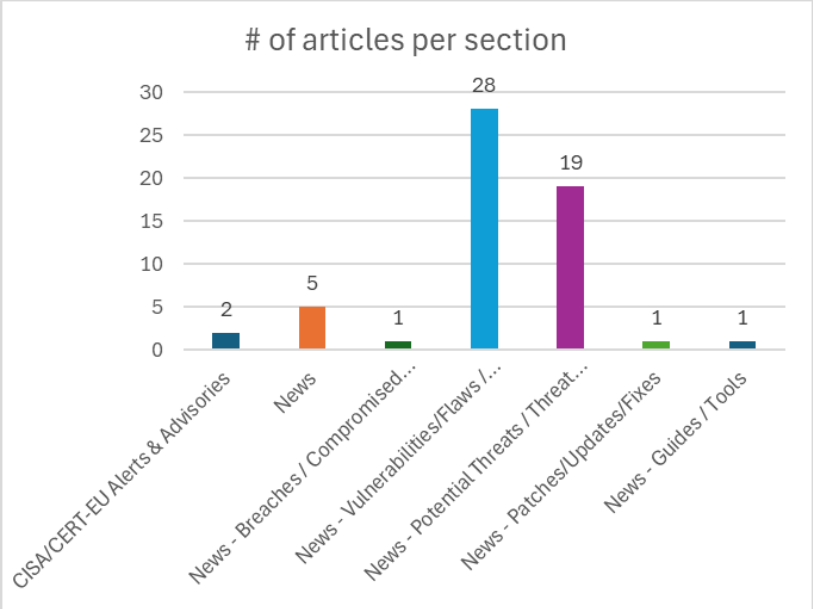
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 13/01/2026 - 16/01/2026





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)	CVSSv 3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2026-23478	10,0	Cal.com	Client-Side Enforcement of Server-Side Security	From 3.1.6 to before 6.0.7	https://github.com/calcom/cal.com/security/advisories/GHSA-7hg4-x4pr-3hrg
https://nvd.nist.gov/vuln/detail/CVE-2026-23550	10,0	Modular DS	Incorrect Privilege Assignment	This issue affects Modular DS: from n/a through 2.5.1	https://help.modulards.com/en/article/modular-ds-security-release-modular-connector-252-dm3mv0/ https://patchstack.com/articles/critical-privilege-escalation-vulnerability-in-modular-ds-plugin-affecting-40k-sites-exploited-in-the-wild/ https://patchstack.com/database/wordpress/plugin/modular-connector/vulnerability/wordpress-modular-ds-monitor-update-and-backup-multiple-websites-plugin-2-5-1-privilege-escalation-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-22907	9,9	SICK	Incorrect Privilege Assignment		https://sick.com/psirt SICK AG https://www.cisa.gov/resources-tools/resources/ics-recommended-practices https://www.first.org/cvss/calculator/3.1 https://www.sick.com/.well-known/csaf/white/2026/sca-2026-0001.json https://www.sick.com/.well-known/csaf/white/2026/sca-2026-0001.pdf https://www.sick.com/media/docs/9/19/719/special_information_sick_operating_guidelines_cyber-security_by_sick_en_im0106719.pdf
https://nvd.nist.gov/vuln/detail/CVE-2025-64155	9.8	Fortinet		FortiSIEM 7.4.0, FortiSIEM 7.3.0 through 7.3.4, FortiSIEM 7.1.0 through	https://fortiguard.fortinet.com/psirt/FG-IR-25-772 https://github.com/horizon3ai/CVE-2025-64155

				7.1.8, FortiSIEM 7.0.0 through 7.0.4, FortiSIEM 6.7.0 through 6.7.10	
https://nvd.nist.gov/vuln/detail/CVE-2026-23746	9,3	Entrust Instant Financial Issuance	Missing Authentication for Critical Function	versions 5.x, prior to 6.10.5	https://trustedcare.entrust.com/s/article/E26-001-NET-Remoting-Vulnerabilities-in-the-Smart-Card-Controller-Service-of-the-Instant-Financial-Issuance-On-Premise-Software https://www.entrust.com/products/issuance-systems/instant/financial-card https://www.vulncheck.com/advisories/entrust-ifi-smartcardcontroller-service-net-remoting-rce
https://nvd.nist.gov/vuln/detail/CVE-2026-22908	9,1	SICK	Incorrect Privilege Assignment		https://sick.com/psirt SICK AG https://www.cisa.gov/resources-tools/resources/ics-recommended-practices https://www.first.org/cvss/calculator/3.1 https://www.sick.com/.well-known/csaf/white/2026/sca-2026-0001.json https://www.sick.com/.well-known/csaf/white/2026/sca-2026-0001.pdf https://www.sick.com/media/docs/9/19/719/special_information_sick_operating_guidelines_cyber-security_by_sick_en_im0106719.pdf
https://nvd.nist.gov/vuln/detail/CVE-2026-23520	9,0	Arcane	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Prior to 1.13.0	https://github.com/getarcaneapp/arcane/commit/5a9c2f92e11f86f8997da8c672844468f930b7e4 https://github.com/getarcaneapp/arcane/pull/1468 https://github.com/getarcaneapp/arcane/releases/tag/v1.13.0 https://github.com/getarcaneapp/arcane/security/advisories/GHSA-gjqq-6r35-w3r8
https://nvd.nist.gov/vuln/detail/CVE-2026-23519	8,9	RustCrypto CMOV	Observable Timing Discrepancy	Prior to 0.4.4	https://github.com/RustCrypto/utils/commit/55977257e7c82a309d5e8abfdd380a774f0f9778 https://github.com/RustCrypto/utils/security/advisories/GHSA-2gqc-6j2q-83qp
https://nvd.nist.gov/vuln/detail/CVE-2026-23527	8,9	H3	Inconsistent Interpretation of HTTP Requests	Prior to 1.15.5	https://github.com/h3js/h3/commit/618ccf4f37b8b6148bea7f36040471af45bfb097 https://github.com/h3js/h3/security/advisories/GHSA-mp2g-9vg9-f4cg

			('HTTP Request/Response Smuggling')		
https://nvd.nist.gov/vuln/detail/CVE-2026-22787	8,7	html2pdf.js	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Prior to 0.14.0	https://github.com/eKoopmans/html2pdf.js/commit/988826e336035b39a8608182d7b73c0e3cd78c7b https://github.com/eKoopmans/html2pdf.js/issues/865 https://github.com/eKoopmans/html2pdf.js/pull/877 https://github.com/eKoopmans/html2pdf.js/releases/tag/v0.14.0 https://github.com/eKoopmans/html2pdf.js/security/advisories/GHSA-w8x4-x68c-m6fc
https://nvd.nist.gov/vuln/detail/CVE-2026-22871	8,7	GuardDog	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Prior to 2.7.1	https://github.com/DataDog/guarddog/commit/9aa6a725b2c71d537d3c18d1c15621395ebb879c https://github.com/DataDog/guarddog/security/advisories/GHSA-xg9w-vg3g-6m68
https://nvd.nist.gov/vuln/detail/CVE-2026-23512	8,6	SumatraPDF	Untrusted Search Path	3.5.2 and earlier	https://github.com/sumatrapdfreader/sumatrapdf/commit/2762e02a8cd7cb779c934a44257aac56ab7de673 https://github.com/sumatrapdfreader/sumatrapdf/security/advisories/GHSA-rqg5-gj63-x4mv
https://nvd.nist.gov/vuln/detail/CVE-2026-22817	8,2	Hono	Improper Verification of Cryptographic Signature	Prior to 4.11.4	https://github.com/honojs/hono/commit/cc0aa7ae327ed84cc391d29086dec2a3e44e7a1f https://github.com/honojs/hono/security/advisories/GHSA-f67f-6cw9-8mq4
https://nvd.nist.gov/vuln/detail/CVE-2026-22864	8,1	Deno	Improper Neutralization of Special Elements used in a Command	Before 2.5.6	https://github.com/denoland/deno/releases/tag/v2.5.6 https://github.com/denoland/deno/security/advisories/GHSA-m3c4-prhw-mrx6

			('Command Injection')		
https://nvd.nist.gov/vuln/detail/CVE-2026-23477	7,7	Rocket	Improper Privilege Management	versions up to 6.12.0	https://github.com/RocketChat/Rocket.Chat/security/advisories/GHSA-g4wm-fg3c-g4p2
https://nvd.nist.gov/vuln/detail/CVE-2026-22910	7,5	SICK	Use of Weak Credentials		https://sick.com/psirt SICK AG https://www.cisa.gov/resources-tools/resources/ics-recommended-practices https://www.first.org/cvss/calculator/3.1 https://www.sick.com/.well-known/csaf/white/2026/sca-2026-0001.json https://www.sick.com/.well-known/csaf/white/2026/sca-2026-0001.pdf https://www.sick.com/media/docs/9/19/719/special_information_sick_operating_guidelines_cyber-security_by_sick_en_im0106719.pdf

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-2026-20805 Microsoft Windows Information Disclosure Vulnerability	https://www.cisa.gov/news-events/alerts/2026/01/13/cisa-adds-one-known-exploited-vulnerability-catalog
Secure Connectivity Principles for Operational Technology (OT)		https://www.cisa.gov/resources-tools/resources/secure-connectivity-principles-operational-technology-ot

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
As Third-Party Vulnerabilities Rise, CISOs Accelerate Push for Security Modernization	https://cybersecuritynews.com/cisos-accelerate-push-for-security-modernization/
Microsoft Warns Secure Boot May Be Bypassed as Windows UEFI Certificates Expire	https://cybersecuritynews.com/windows-secure-boot-certificates-expire/
New Android Bug Impacts Volume Buttons Functionality with “Select to Speak” Enabled	https://cybersecuritynews.com/android-bug-impacts-volume-buttons-function/
10 Best ISO 27001 Compliant Security Companies – 2026	https://cybersecuritynews.com/iso-27001-compliant-companies/
5 SOC Challenges You Can Eliminate with a Single Improvement	https://cybersecuritynews.com/5-soc-challenges-you-can-eliminate-with-a-single-improvement/

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
Betterment Confirms that Hackers Gained Access to Internal Systems	https://cybersecuritynews.com/betterment-confirms-hackers-access/

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
Cisco 0-Day RCE Secure Email Gateway Vulnerability Exploited in the Wild	https://cybersecuritynews.com/cisco-0-day-rce-secure-email-gateway-vulnerability/
Go 1.25.6 and 1.24.12 Patch Critical Vulnerabilities Lead to DoS and Memory Exhaustion Risks	https://cybersecuritynews.com/go-1-25-6-and-1-24-12-vulnerabilities/
New AWS Console Supply Chain Attack Lets Attackers Hijack AWS GitHub Repositories	https://cybersecuritynews.com/aws-console-supply-chain-attack/
Fortinet FortiSIEM Vulnerability CVE-2025-64155 Actively Exploited in Attacks	https://cybersecuritynews.com/fortinet-fortisiem-vulnerability/
Azure Identity Token Vulnerability Enables Tenant-Wide Compromise in Windows Admin Center	https://cybersecuritynews.com/azure-identity-token-vulnerability/
Windows Remote Assistance Vulnerability Allow Attacker to Bypass Security Features	https://cybersecuritynews.com/windows-remote-assistance-vulnerability/
Critical Cal.com Vulnerability Let Attackers Bypass Authentication and Hijack any User Account	https://cybersecuritynews.com/cal-com-vulnerability-bypass-authentication/
Firefox 147 Released With Fixes for 16 Vulnerabilities that Enable Arbitrary Code Execution	https://cybersecuritynews.com/firefox-147-released/
Critical WordPress Plugin Vulnerability Exploited in the Wild to Gain Instant Admin Access	https://cybersecuritynews.com/wordpress-plugin-vulnerability-admin-access/
HPE Aruba Vulnerabilities Enables Unauthorized Access to Sensitive Information	https://cybersecuritynews.com/hpe-aruba-vulnerabilities/
Chinese Threat Actors Hosted 18,000 Active C2 Servers Across 48 Hosting Providers	https://cybersecuritynews.com/chinese-threat-actors-hosted-18000-active-c2-servers/
Palo Alto Networks Firewall Vulnerability Allows Attacker to Trigger DoS Attacks	https://cybersecuritynews.com/palo-alto-networks-firewall-dos-vulnerability/
Microsoft SQL Server Vulnerability Allows Attackers to Elevate Privileges over a Network	https://cybersecuritynews.com/microsoft-sql-server-eol-vulnerability/
New One-Click Microsoft Copilot Vulnerability Grants Attackers Undetected Access to Sensitive Data	https://cybersecuritynews.com/reprompt-single-click-copilot-exploit/

Critical FortiSIEM Vulnerability(CVE-2025-64155) Enable Full RCE and Root Compromise	https://cybersecuritynews.com/fortisiem-vulnerability-rce/
Critical FortiSIEM Vulnerability Enables Arbitrary Commands Execution via Crafted TCP Packets	https://cybersecuritynews.com/fortisiem-vulnerability/
Spring CLI Tool Vulnerability Enables Command Execution on the Users Machine	https://cybersecuritynews.com/spring-cli-tool-vulnerability/
Elastic Patches Multiple Vulnerabilities That Enables Arbitrary File Theft and DoS Attacks	https://cybersecuritynews.com/elastic-patches-multiple-vulnerabilities/
Chrome 144 Released With Fix for 10 Vulnerabilities in V8 JavaScript Engine	https://cybersecuritynews.com/chrome-144-released/
Microsoft Desktop Window Manager 0-Day Vulnerability Exploited in the wild	https://cybersecuritynews.com/desktop-window-manager-0-day-vulnerability/
Microsoft Patch Tuesday January 2026 – 114 Vulnerabilities Fixed Including 3 Zero-days	https://cybersecuritynews.com/microsoft-patch-tuesday-january-2026/
FortiSandbox SSRF Vulnerability Allow Attacker to proxy Internal Traffic via Crafted HTTP Requests	https://cybersecuritynews.com/fortisandbox-ssrf-vulnerability/
FortiOS and FortiSwitchManager Vulnerability Let Remote Attackers Execute Arbitrary Code	https://cybersecuritynews.com/fortios-and-fortiswitchmanager-vulnerability/
Critical ServiceNow Vulnerability Enables Privilege Escalation Via Unauthenticated User Impersonation	https://cybersecuritynews.com/servicenow-vulnerability/
CISA Warns of Gogs Path Traversal Vulnerability Exploited in Attacks	https://cybersecuritynews.com/cisa-gogs-path-traversal-vulnerability/
New Angular Vulnerability Enables an Attacker to Execute Malicious Payload	https://cybersecuritynews.com/angular-vulnerability/
100,000+ n8n Instances Exposed to Internet Vulnerable to RCE Attacks	https://cybersecuritynews.com/100000-n8n-instances-exposed/
Multiple Hikvision Vulnerabilities Let Attackers Cause Device Malfunction Using Crafted Packets	https://cybersecuritynews.com/multiple-hikvision-lan-vulnerabilities/

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
Node.js Security Release Patches 7 Vulnerabilities Across All Release Lines	https://cybersecuritynews.com/node-js-security-release/

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
Hackers Abusing Legitimate Cloud and CDN Platforms to Host Phishing Kits	https://cybersecuritynews.com/hackers-abusing-legitimate-cloud/
Promptware Kill Chain – Five-Step Kill Chain Model for Analyzing Cyberthreats	https://cybersecuritynews.com/promptware-kill-chain-five-step-kill-chain-model/
MonetaStealer Malware Powered with AI Code Attacking macOS Users in the Wild	https://cybersecuritynews.com/monetastealer-malware-powered/
New Sicarii RaaS Operation Attacks Exposed RDP Services and Attempts to Exploit Fortinet Devices	https://cybersecuritynews.com/new-sicarii-raas-operation-attacks-exposed-rdp-services/
Turla's Kazuar v3 Loader Leverages Event Tracing for Windows and Bypasses Anti-malware Scan Interface	https://cybersecuritynews.com/turlas-kazuar-v3-loader-leverages-event-tracing/
Microsoft and Authorities Dismatles BEC Attack Chain Powered by RedVDS Fraud Engine	https://cybersecuritynews.com/microsoft-and-authorities-dismatles-bec-attack-chain/
Researchers Breakdown DragonForce Ransomware Along with Decryptor for ESXi and Windows Systems	https://cybersecuritynews.com/researchers-breakdown-dragonforce-ransomware/
North Korean Hackers use Code Abuse Tactics for 'Contagious Interview' Campaign	https://cybersecuritynews.com/north-korean-hackers-use-code-abuse-tactics/
LLMs are Accelerating the Ransomware Lifecycle to Gain Speed, Volume, and Multi-lingual Reach	https://cybersecuritynews.com/llms-are-accelerating-the-ransomware-lifecycle/
New Magecart Attack Steals Customers Credit Cards from Website Checkout Pages	https://cybersecuritynews.com/new-magecart-attack-steals-customers-credit-cards/
Multi-Stage Windows Malware Invokes PowerShell Downloader Using Text-based Payloads Using Remote Host	https://cybersecuritynews.com/multi-stage-windows-malware-invokes-powershell-downloader/
HoneyTrap – A New LLM Defense Framework to Counter Jailbreak Attacks	https://cybersecuritynews.com/honeytrap-a-new-llm-defense-framework/
Critical OpenSSH Vulnerability Exposes Moxa Ethernet Switches to Remote Code Execution	https://cybersecuritynews.com/moxa-ethernet-switches-openssh/
Android Banking Malware deVixor Actively Targeting Users with Ransomware Capabilities	https://cybersecuritynews.com/android-banking-malware-devixor-actively-targeting-users/
Threat Actors Leveraging RMM Tools to Attack Users via Weaponized PDF Files	https://cybersecuritynews.com/threat-actors-leveraging-rmm-tools/
New VoidLink Cloud-Native Malware Attacking Linux Systems with Self-deletion Capabilities	https://cybersecuritynews.com/new-voidlink-cloud-native-malware/
Hackers Leverage Browser-in-the-browser Tactic to Trick Facebook Users and Steal Logins	https://cybersecuritynews.com/hackers-leverage-browser-in-the-browser-tactic/
AsyncRAT Leveraging Cloudflare's Free-Tier Services to Mask Malicious Activities and Detection	https://cybersecuritynews.com/asyncrat-leveraging-cloudflares-free-tier-services/
Malicious Chrome Extension Steals Wallet Login Credentials and Enables Automated Trading	https://cybersecuritynews.com/malicious-chrome-extension-steals-wallet-login-credentials/

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
AuraAudit – Open-Source Tool for Salesforce Aura Framework Misconfiguration Analysis	https://cybersecuritynews.com/aurainspector-audit-salesforce/

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/