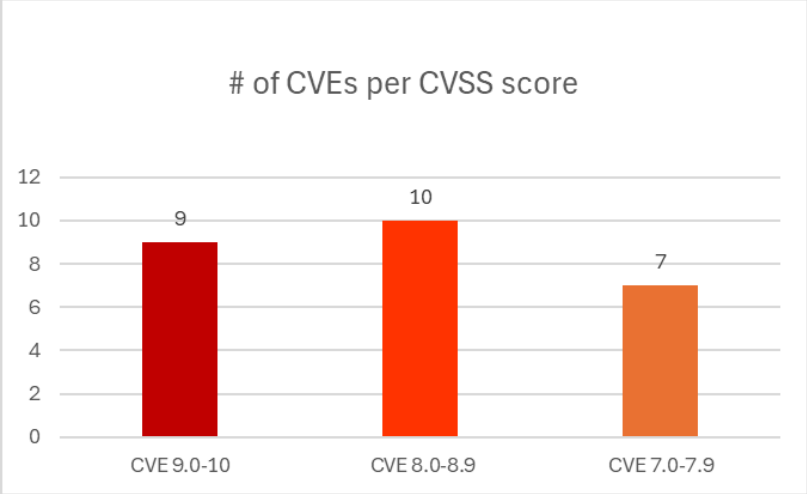
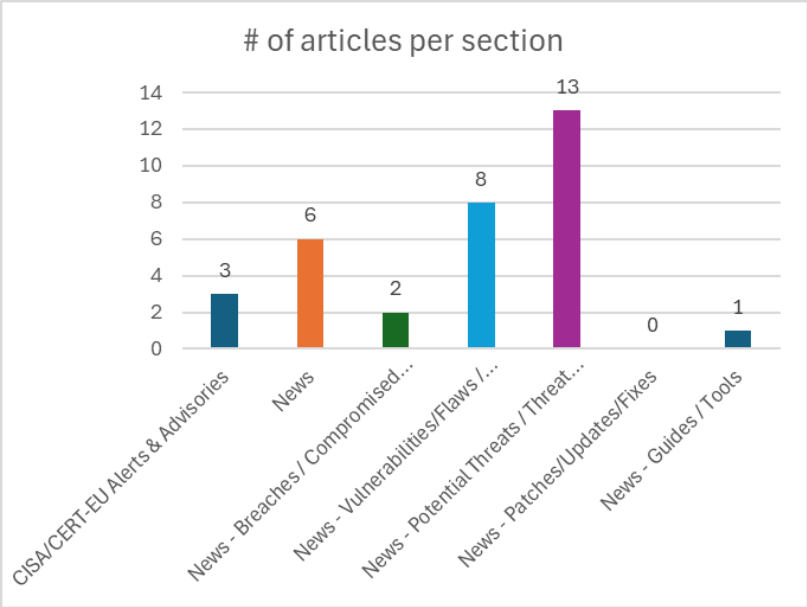
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 27/06/2026 - 30/06/2026





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)	CVSS v3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2026-48558	10,0	SimpleHelp	Improper Verification of Cryptographic Signature	SimpleHelp versions 5.5.15 and prior and 6.0 pre-release versions	https://blackpointcyber.com/blog/a-djinn-in-the-machine-taskweavers-node-js-intrusion-chain/ https://horizon3.ai/attack-research/disclosures/cve-2026-48558-simple-help-authentication-bypass-iocs/ https://simple-help.com/release-news https://simple-help.com/security/simplehelp-security-update-2026-05 https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-48558
https://nvd.nist.gov/vuln/detail/CVE-2026-57331	9,9	Videochat Turnkey Site	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Performer Arbitrary File Deletion in Paid Videochat Turnkey Site <= 7.4.8 versions	https://patchstack.com/database/wordpress/plugin/ppv-live-webcams/vulnerability/wordpress-paid-videochat-turnkey-site-plugin-7-4-8-arbitrary-file-deletion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-58053	9,9	Gitea	Improper Privilege Management	Gitea act_runner with the Docker backend (through act 0.262.0)	https://github.com/bikini/exploitarium/tree/main/gitea-act-runner-container-options-poc https://www.vulncheck.com/advisories/gitea-act-runner-container-hardening-bypass-via-workflow-container-options
https://nvd.nist.gov/vuln/detail/CVE-2026-13762	9,8	Amazon CloudFront	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')	Amazon CloudFront with AWS WAF enabled	https://aws.amazon.com/security/security-bulletins/2026-048-aws/
https://nvd.nist.gov/vuln/detail/CVE-2026-13763	9,8	AWS Application Load Balancer	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')	Inconsistent interpretation of HTTP/2 requests in AWS Application Load Balancer with AWS WAF enabled	https://aws.amazon.com/security/security-bulletins/2026-048-aws/ https://docs.aws.amazon.com/elasticloadbalancing/latest/application/edit-target-group-attributes.html#waf-http2-inspection
https://nvd.nist.gov/vuln/detail/CVE-2026-49048	9,8	Joomla extension JoomCCK	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Joomla extension JoomCCK	https://www.joomcoder.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-56782	9,8	Gorse	Missing Authentication for Critical Function	Gorse before 0.5.10	https://github.com/gorse-io/gorse/commit/19fdcbb309fb5b609e9cc3eb10c74885b5b27da9 https://github.com/gorse-io/gorse/issues/1292 https://github.com/gorse-io/gorse/pull/1293 https://www.vulncheck.com/advisories/gorse-unauthenticated-database-dump-and-restore-via-api-dump-and-api-restore-endpoints
https://nvd.nist.gov/vuln/detail/CVE-2026-57498	9,6	Coolify	Authorization Bypass Through User-Controlled Key	Prior to 4.0.0-beta.474	https://github.com/coollabsio/coolify/security/advisories/GHSA-725v-f5gh-22q9

https://nvd.nist.gov/vuln/detail/CVE-2026-37637	9,1	Alexantr filemanager	Improper Control of Generation of Code ('Code Injection')	Alexantr filemanager v.1.0	https://github.com/SLO-CYBER-SEC/CVE-2026-37637
https://nvd.nist.gov/vuln/detail/CVE-2026-12856	8,8	vscode-java extension	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	A flaw was found in the vscode-java extension, which provides Java language support for Visual Studio Code	https://access.redhat.com/security/cve/CVE-2026-12856 https://bugzilla.redhat.com/show_bug.cgi?id=2491278 https://github.com/redhat-developer/vscode-java/security/advisories/GHSA-7qv8-6qrw-3crv https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-12856.json
https://nvd.nist.gov/vuln/detail/CVE-2026-13519	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda JD12L 16.03.53.23	https://github.com/cve-a/Yuanji-Wanshu/issues/1 https://vuldb.com/cve/CVE-2026-13519 https://vuldb.com/submit/838993 https://vuldb.com/vuln/374527 https://vuldb.com/vuln/374527/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-13539	8,8	Wavlink	Improper Restriction of Operations within the Bounds of a Memory Buffer	Wavlink WL-NU516U1-A M16U1_V240425	https://dl.wavlink.com/firmware/RD/WINSTAR_NU516U1-WO-A-2026-06-22-5ccde97-mt7628-squashfs-sysupgrade.bin https://github.com/Svigo-o/Wavlink_vul/tree/main/wavlink-wl-nu516u1-wireless-guestwifi-guestssid-buffer-overflow https://vuldb.com/cve/CVE-2026-13539 https://vuldb.com/submit/834024 https://vuldb.com/vuln/374547 https://vuldb.com/vuln/374547/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-13545	8,8	D-Link	Improper Neutralization of Special Elements used in a Command ('Command Injection')	D-Link DCS-935L 1.10.01	https://github.com/Real-Simplicity/cve-database/tree/main/CVE_Report_DLink_DCS935L_Command_Injection https://vuldb.com/cve/CVE-2026-13545 https://vuldb.com/submit/842589 https://vuldb.com/vuln/374553 https://vuldb.com/vuln/374553/cti https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-13583	8,8	Edimax	Improper Restriction of Operations within the Bounds of a Memory Buffer	A vulnerability has been found in Edimax EW-7478APC 1.04	https://lavender-bicycle-a5a.notion.site/EDIMAX-EW-7478APC-for-mUSBFolder-34b53a41781f80d5b1f8ebce442de53f https://vuldb.com/cve/CVE-2026-13583 https://vuldb.com/submit/844118 https://vuldb.com/vuln/374589 https://vuldb.com/vuln/374589/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-34594	8,8	Coolify	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Prior to 4.0.0-beta.471	https://github.com/coollabsio/coolify/security/advisories/GHSA-mf8p-rj62-9f9m
https://nvd.nist.gov/vuln/detail/CVE-2026-43731	8,8	Apple Inc.	Use After Free	This issue is fixed in Safari 26.5.2, iOS 26.5.2 and iPadOS 26.5.2, macOS Tahoe 26.5.2	https://support.apple.com/en-us/127594 https://support.apple.com/en-us/127595 https://support.apple.com/en-us/127685
https://nvd.nist.gov/vuln/detail/CVE-2026-58000	8,8	luci-proto-openvpn	Improper Neutralization of Special Elements used in	luci-proto-openvpn through 0.11.1	https://github.com/openwrt/luci/commit/e4ff45ecbc6ad212951815c8c99b2749fbd7de6b

			an OS Command ('OS Command Injection')		https://github.com/openwrt/luci/security/advisories/GHSA-pm9w-522m-8rrh https://www.vulncheck.com/advisories/luci-proto-openvpn-command-injection-via-cl-meta-parameter-in-generatekey
https://nvd.nist.gov/vuln/detail/CVE-2026-58049	8,6	FFmpeg's RASC video decoder	Out-of-bounds Write	-	https://access.redhat.com/security/cve/CVE-2026-58049 https://bugzilla.redhat.com/show_bug.cgi?id=2493952 https://github.com/FFmpeg/FFmpeg/blob/master/libavcodec/rasc.c https://github.com/bikini/exploitarium/tree/main/ffmpeg-rasc-dlta-calc-poc https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-58049.json https://www.vulncheck.com/advisories/ffmpeg-out-of-bounds-write-in-rasc-decoder-decode-dlta
https://nvd.nist.gov/vuln/detail/CVE-2026-58302	8,4	LinuxCNC	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	LinuxCNC before 2.9.9	https://bugs.debian.org/1140943 https://github.com/LinuxCNC/linuxcnc/commit/00d534c87464a3ed446656998aa02b8abc74b391 https://github.com/LinuxCNC/linuxcnc/commit/ea7cd579d39b586952a42e3da9a26d3e36e7a272 https://github.com/LinuxCNC/linuxcnc/compare/v2.9.8...v2.9.9
https://nvd.nist.gov/vuln/detail/CVE-2026-49412	7,8	FreeBSD	Use After Free	The kernel handler for IPV6_MSFILTER dropped a serializing lock in order to copy the source-filter list from userspace, then reacquired the lock.	https://security.freebsd.org/advisories/FreeBSD-SA-26:29.ip6_multicast.asc
https://nvd.nist.gov/vuln/detail/CVE-2026-57919	7,8	PBack-upVSS.exe in Matrix42 Empirum	Incorrect Default Permissions	PBackupVSS.exe in Matrix42 Empirum before 25.5 and 26.x before 26.2	https://docs.matrix42.com/en_US/1041748_vulnerability-list/cve-2026-57919-privilege-escalation-in-empirum-personal-backup https://matrix42.com
https://nvd.nist.gov/vuln/detail/CVE-2026-8023	7,5	Zephyr's HTTP server	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Affects releases v4.0.0 through v4.4.0 for deployments that register a static-filesystem resource	https://github.com/zephyrproject-rtos/zephyr/commit/f4a423c98554f209c5d2f22f041822422c9263b8 https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-hch3-53g6-jj3h
https://nvd.nist.gov/vuln/detail/CVE-2026-10646	7,4	Zephyr Project	Use After Free	Zephyr's BSD-sockets getaddrinfo() implementation (subsys/net/lib/sockets/getaddrinfo.c)	https://github.com/zephyrproject-rtos/zephyr/commit/cd27da58eedb8d0fe380dd340b81ca5afa35de45 https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-h752-vhmf-29w6
https://nvd.nist.gov/vuln/detail/CVE-2026-22078	7,3	OPPO Mobile Telecommunication Corp., Ltd.	Incorrect Privilege Assignment	Because O+ Connect's IPC service does not authenticate clients, external applications can escalate privileges and perform sensitive actions through the IPC channel.	https://security.oppo.com/en/noticeDetail?notice_only_key=NOTICE-2070415238859333632
https://nvd.nist.gov/vuln/detail/CVE-2026-13601	7,1	Red Hat, Inc.	Protection Mechanism Failure	A flaw was found in Yelp due to an overly permissive Content Security Policy (CSP) implementation provided by yelp-xsl.	https://access.redhat.com/security/cve/CVE-2026-13601 https://blogs.gnome.org/mcatanzaro/2026/05/11/flatpak-sandbox-escape-via-yelp/ https://bugzilla.redhat.com/show_bug.cgi?id=2494110 https://gitlab.gnome.org/GNOME/yelp/-/commit/c8c8244c8a812860782d635890c9b6c43ecc2639

					https://gitlab.gnome.org/GNOME/yelp/-/work_items/238 https://security.access.redhat.com/data/csaf/v2/vex/2026/cve-2026-13601.json
https://nvd.nist.gov/vuln/detail/CVE-2026-49413	**7,1**	Linuxulator	Incorrect Privilege Assignment	-	https://security.freebsd.org/advisories/FreeBSD-SA-26:30.linux.asc

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
Russian Intelligence Services Continue to Target Commercial Messaging Applications		https://www.cisa.gov/resources-tools/resources/russian-intelligence-services-continue-target-commercial-messaging-applications
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2026-48558 SimpleHelp Authentication Bypass Vulnerability	https://www.cisa.gov/news-events/alerts/2026/06/29/cisa-adds-one-known-exploited-vulnerability-catalog
Vulnerability Summary for the Week of June 22, 2026		https://www.cisa.gov/news-events/bulletins/sb26-180

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
WhatsApp Launches New Username Feature to Communicate Without Exposing Phone Numbers	https://cybersecuritynews.com/whatsapp-username-feature-2/
Russia-Linked Turla Uses Compromised Infrastructure to Deploy STOCKSTAY in Ukraine Operations	https://cybersecuritynews.com/russia-linked-turla-uses-compromised-infrastructure/
LLM-Generated Mythic Agents Enable Disposable Red-Team Tooling From Prompt to Deployment	https://cybersecuritynews.com/llm-generated-mythic-agents-enable-disposable-red-team-tooling/
China’s New Zhipu AI Reportedly Matches Claude Mythos in Vulnerability Detection	https://cybersecuritynews.com/zhipu-ai-vulnerability-detection/
OpenAI Released GPT-5.6 Sol With Limited Access and Strong Cyberattack Protections	https://cybersecuritynews.com/gpt-5-6-release/
Hackers Exploit Weak Credentials and Internet-Facing PLCs to Breach Water Utilities	https://cybersecuritynews.com/hackers-exploit-weak-credentials-and-internet-facing-plcs/

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
Nissan Confirms Data Breach Following Oracle PeopleSoft 0-Day Attacks	https://cybersecuritynews.com/nissan-confirms-data-breach/
EvilTokens Phishing Breaches Finance Firms Using “Ghost” Code Across U.S. and European Businesses	https://cybersecuritynews.com/eviltokens-phishing-breaches-finance-firms-using-ghost-code-across-u-s-and-european-businesses/

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
Public PoC Released for Deserialization RCE Vulnerability in Splunk Secure Gateway	https://cybersecuritynews.com/splunk-secure-gateway-deserialization-rce-vulnerability/
Critical Dell Wyse Vulnerabilities Enable Remote Code Execution Attacks	https://cybersecuritynews.com/dell-wyse-vulnerabilities/
Microsoft 365 Apps RCE Vulnerability Exploited Using a Malicious Excel File	https://cybersecuritynews.com/microsoft-365-apps-rce-vulnerability-exploit/
Critical Gemini CLI Vulnerability Lets Attackers Execute Arbitrary Code	https://cybersecuritynews.com/critical-gemini-cli-vulnerability/
New DirtyClone Linux Vulnerability Allows Attackers to Gain Root Access Via Cloned Packets	https://cybersecuritynews.com/dirtyclone-linux-vulnerability/
Amazon Q Vulnerability Let Attackers Execute Code and Access Sensitive Cloud Environments	https://cybersecuritynews.com/amazon-q-vulnerability/
New Linux pedit COW Exploit Allows Attackers to Gain System Root Access	https://cybersecuritynews.com/linux-pedit-cow-exploit/
Critical python.org Vulnerability Allowed Attackers to Forge Admin-Level API Requests	https://cybersecuritynews.com/critical-python-org-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

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
New Claude Code Attack Allows Attackers to Take Full Control of Developers' Sys-tems	https://cybersecuritynews.com/new-claude-code-attack/
Hackers Exploiting Critical Oracle E-Business Suite Vulnerability Actively in Attacks	https://cybersecuritynews.com/oracle-e-business-flaw-actively-exploited/
ClawHub Skills Expose AI Agents to Remote Control Backdoors and Data Theft At-tacks	https://cybersecuritynews.com/clawhub-skills-expose-ai-agents/
Hackers Could Abuse WM_COPYDATA Callback Path to Execute Code Through Win32k Dispatch	https://cybersecuritynews.com/hackers-could-abuse-wm_copydata-callback-path/
DCloud Uni-App Scam Network Powers RainbowEx-Style Crypto Fraud and WhatsApp Phishing	https://cybersecuritynews.com/dcloud-uni-app-scam-network-powers-rainbowex-style-crypto-fraud/
Millenium RAT Rewritten in C++ Infects 62,000+ Devices Across 160 Countries	https://cybersecuritynews.com/millenium-rat-rewritten-in-c/
Hackers Use Rokarolla Banking Trojan to Intercept SMS Codes and Steal Crypto Cre-dentials	https://cybersecuritynews.com/hackers-use-rokarolla-banking-trojan-to-intercept-sms-codes/
New Bucket Hijacking Attack Allows Hackers to Reroute Cloud Data Streams to Ex-ternal Storage	https://cybersecuritynews.com/bucket-hijacking-attack/
New Bluekit Phishing-as-a-Service Bypasses MFA to Steal Microsoft Login Creden-tials	https://cybersecuritynews.com/bluekit-paas-bypasses-mfa/
New GIFTEDCROOK Chain Abuses WinRAR ADS and Reflective Loading to Steal Browser Data	https://cybersecuritynews.com/new-giftedcrook-chain-abuses-winrar-ads/
Hackers Leveraged Shopify Oder-Tracking App Shop to Push Fake Invoices	https://cybersecuritynews.com/hackers-leveraged-shopify-oder-tracking-app-shop/
KuinaExtractor Uses Telegram Exfiltration, UAC Bypass, and Sandbox Detection for Stealth	https://cybersecuritynews.com/kuinaextractor-uses-telegram-exfiltration/
Miasma Malware Uses binding.gyp and Bun to Execute Hidden Payloads in npm Packages	https://cybersecuritynews.com/miasma-malware-uses-binding-gyp-and-bun/

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 επαγ-γελματιών ασφάλειας.

Σύντομη περιγραφή / Τίτλος	URL
RedAmon AI Tool that Chains Reconnaissance, Exploitation, and Post-exploitation	https://cybersecuritynews.com/redamon-ai-tool/

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/