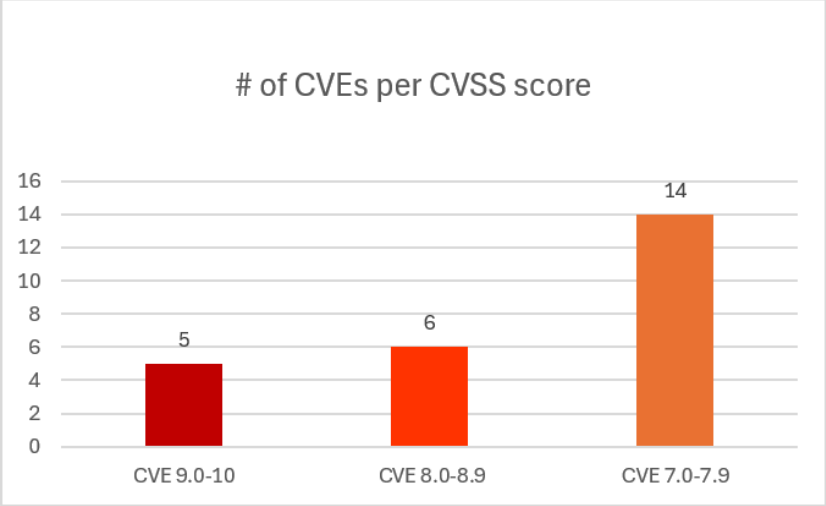
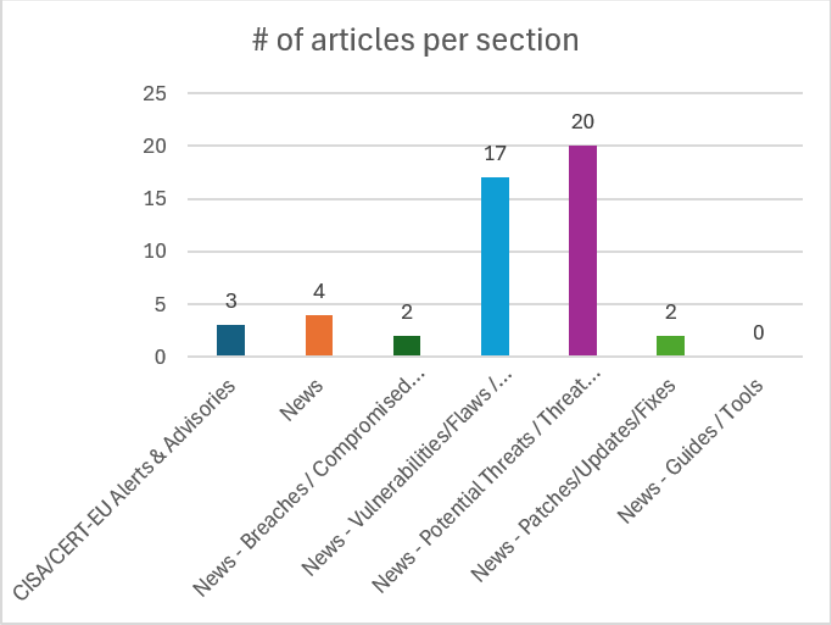
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 10/06/2026 - 12/06/2026





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-2026-49261	10,0	MariaDB server	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Versions 10.6.1 through 10.6.26, 10.11.1 through 10.11.17, 11.4.1 through 11.4.11, 11.8.1 through 11.8.7, and 12.3.1 with `wsrep_notify_cmd` enabled would execute shell commands embedded in the name of the joiner node. This is fixed in 10.6.27, 10.11.18, 11.4.12, 11.8.8, and 12.3.2. As a workaround, anyone who cannot upgrade now should disable `wsrep_notify_cmd`.	https://github.com/MariaDB/server/security/advisories/GHSA-3p3m-4x7c-p4pw https://jira.mariadb.org/browse/MDEV-39721
https://nvd.nist.gov/vuln/detail/CVE-2026-47370	9,9	UniFi OS	Improper Input Validation	-	https://community.ui.com/releases/Security-Advisory-Bulletin-065-065/aa46a22b-fc43-4eae-9382-6fc8feda967a
https://nvd.nist.gov/vuln/detail/CVE-2026-20253	9,8	Splunk Enterprise	Missing Authentication for Critical Function	In Splunk Enterprise versions below 10.2.4 and 10.0.7, and Splunk Cloud Platform versions below 10.4.2604.3 and 10.2.2510.14	https://advisory.splunk.com/advisories/SVD-2026-0603
https://nvd.nist.gov/vuln/detail/CVE-2026-46703	9,6	Boxlite	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Prior to version 0.9.0	https://github.com/boxlite-ai/boxlite/releases/tag/v0.9.0 https://github.com/boxlite-ai/boxlite/security/advisories/GHSA-f396-4rp4-7v2j
https://nvd.nist.gov/vuln/detail/CVE-2026-9648	9,1	Haskell library	-	The crypton-x509-validation Haskell library fails to enforce X.509 NameConstraints	https://github.com/haskell/security-advisories/pull/332 https://github.com/kazu-yamamoto/crypton-certificate/pull/30 https://github.com/kazu-yamamoto/crypton-certificate/pull/30/changes/f4b77edf6ead77f4a886da40e41eab20f0180e39 https://hackage.haskell.org/package/crypton-x509-validation-1.9.1/revisions/ https://www.kb.cert.org/vuls/id/862559
https://nvd.nist.gov/vuln/detail/CVE-2026-11933	8,8	MongoDB	Out-of-bounds Write	-	https://jira.mongodb.org/browse/SERVER-128125
https://nvd.nist.gov/vuln/detail/CVE-2026-53435	8,8	Jenkins	Deserialization of Untrusted Data	In Jenkins 2.567 and earlier, LTS 2.555.2 and earlier	https://www.jenkins.io/security/advisory/2026-06-10/#SECURITY-3707
https://nvd.nist.gov/vuln/detail/CVE-2026-7870	8,8	IBM	Uncontrolled Search Path Element	IBM i 7.6, 7.5, 7.4, and 7.3	https://www.ibm.com/support/pages/node/7275756

https://nvd.nist.gov/vuln/detail/CVE-2026-10087	8,7	GitLab	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	in GitLab EE affecting all versions from 17.1 before 18.10.8, 18.11 before 18.11.5, and 19.0 before 19.0.2	https://about.gitlab.com/releases/2026/06/10/patch-release-gitlab-19-0-2-released/ https://gitlab.com/gitlab-org/gitlab/-/work_items/601633 https://hackerone.com/reports/3759090
https://nvd.nist.gov/vuln/detail/CVE-2026-8589	8,7	GitLab	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	all versions from 13.1.4 before 18.10.8, 18.11 before 18.11.5, and 19.0 before 19.0.2	https://about.gitlab.com/releases/2026/06/10/patch-release-gitlab-19-0-2-released/ https://gitlab.com/gitlab-org/gitlab/-/work_items/600099 https://hackerone.com/reports/3722842
https://nvd.nist.gov/vuln/detail/CVE-2026-12034	8,3	Google Chrome	Improper Input Validation	in Linux Toolkit Theming in Google Chrome on Linux prior to 149.0.7827.115	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_01962725236.html https://issues.chromium.org/issues/519258799
https://nvd.nist.gov/vuln/detail/CVE-2025-31272	7,8	Apple Inc.	Improper Privilege Management	This issue is fixed in macOS Sequoia 15.4	https://support.apple.com/en-us/122373
https://nvd.nist.gov/vuln/detail/CVE-2026-52755	7,8	Ghidra	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Ghidra before 12.0.4	https://github.com/NationalSecurityAgency/ghidra/security/advisories/GHSA-3r55-xjr4-jh8f https://www.vulncheck.com/advisories/ghidra-path-traversal-via-zip-slip-in-theme-import
https://nvd.nist.gov/vuln/detail/CVE-2026-9045	7,8	Lenovo Accessories and Display Manager	Missing Authentication for Critical Function	Lenovo Accessories and Display Manager for Enterprise for Windows	https://support.lenovo.com/us/en/downloads/ds568567 https://support.lenovo.com/us/en/product_security/LEN-213623
https://nvd.nist.gov/vuln/detail/CVE-2026-50245	7,7	Brickcom	Missing Authentication for Critical Function	Brickcom cameras	https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-162-03.json https://www.brickcom.com/case/ https://www.cisa.gov/news-events/ics-advisories/icsa-26-162-03
https://nvd.nist.gov/vuln/detail/CVE-2025-46315	7,5	Apple Inc.	Improper Access Control	This issue is fixed in macOS Tahoe 26.1	https://support.apple.com/en-us/125634
https://nvd.nist.gov/vuln/detail/CVE-2026-10143	7,5	kafka-python	Uncontrolled Resource Consumption	kafka-python prior to 2.3.2	https://github.com/dpkp/kafka-python/commit/6e4831444f972d169cdd11f5c8d50333cea3f19b https://github.com/dpkp/kafka-python/pull/3019 https://github.com/dpkp/kafka-python/pull/3026 https://www.vulncheck.com/advisories/kafka-python-prior-to-dos-via-scram-iteration-count-in-scram-py

https://nvd.nist.gov/vuln/detail/CVE-2026-1220	7,5	Google Chrome	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	Race in V8 in Google Chrome prior to 144.0.7559.99	https://chromereleases.google-blog.com/2026/01/stable-channel-update-for-desktop_20.html https://issues.chromium.org/issues/473851441
https://nvd.nist.gov/vuln/detail/CVE-2026-41856	7,5	Spring GraphQL	Improper Access Control	Affected versions: Spring for GraphQL 2.0.0 through 2.0.3; 1.4.0 through 1.4.5; 1.3.0 through 1.3.8; 1.0.0 through 1.0.6.	https://spring.io/security/cve-2026-41856
https://nvd.nist.gov/vuln/detail/CVE-2026-44496	7,5	Axios	Uncontrolled Resource Consumption	Axios versions before 0.32.0 on the 0.x line and before 1.16.0 on the 1.x line	https://github.com/axios/axios/security/advisories/GHSA-hfxv-24rg-xrqf
https://nvd.nist.gov/vuln/detail/CVE-2026-44890	7,5	Netty	Uncontrolled Resource Consumption	prior to versions 4.1.135.Final and 4.2.15	https://github.com/netty/netty/releases/tag/netty-4.1.135.Final https://github.com/netty/netty/releases/tag/netty-4.2.15.Final https://github.com/netty/netty/security/advisories/GHSA-6ghj-frrj-jjj3
https://nvd.nist.gov/vuln/detail/CVE-2026-7250	7,5	GitLab	Allocation of Resources Without Limits or Throttling	all versions from 12.10 before 18.10.8, 18.11 before 18.11.5, and 19.0 before 19.0.2	https://about.gitlab.com/releases/2026/06/10/patch-release-gitlab-19-0-2-released/ https://gitlab.com/gitlab-org/gitlab/-/work_items/598311 https://hackerone.com/reports/3671995
https://nvd.nist.gov/vuln/detail/CVE-2026-7787	7,5	IBM	Authorization Bypass Through User-Controlled Key	IBM Langflow OSS 1.0.0 through 1.9.1	https://www.ibm.com/support/pages/node/7275453
https://nvd.nist.gov/vuln/detail/CVE-2022-26758	7,1	Apple Inc.	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	This issue is fixed in macOS Monterey 12.4	https://support.apple.com/en-us/102871 https://support.apple.com/en-us/213257
https://nvd.nist.gov/vuln/detail/CVE-2026-6090	7,0	Lenovo	Authentication Bypass by Spoofing	Lenovo Smart Connect for Windows	https://support.lenovo.com/us/en/product_security/LEN-218281

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-2026-42271 BerriAI LiteLLM Command Injection Vulnerability ▪ CVE-2026-50751 Check Point Security Gateway Improper Authentication Vulnerability	https://www.cisa.gov/news-events/alerts/2026/06/08/cisa-adds-two-known-exploited-vulnerabilities-catalog
CISA Adds Three Known Exploited Vulnerabilities to Catalog	▪ CVE-2026-7473 Arista Extensible Operating System Incomplete Comparison with Missing Factors Vulnerability ▪ CVE-2026-11645 Google Chromium V8 Out-of-Bounds Read and Write Vulnerability ▪ CVE-2026-20245 Cisco Catalyst SD-WAN Manager Improper Encoding or Escaping of Output Vulnerability	https://www.cisa.gov/news-events/alerts/2026/06/09/cisa-adds-three-known-exploited-vulnerabilities-catalog
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2026-10520 Ivanti Sentry OS Command Injection Vulnerability	https://www.cisa.gov/news-events/alerts/2026/06/11/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
Authorities Dismantle Cryptocurrency Laundering Services ‘AudiA6’ Used by Ransomware Gangs	https://cybersecuritynews.com/authorities-dismantle-audia6-services/
GitHub to Automate Disable npm Script Installs to Block Supply Chain Attacks	https://cybersecuritynews.com/github-automated-disable-npm-script-installs/
Claude Mythos Turning N-Days Into N-Hours With Rapid Working Exploit Creation	https://cybersecuritynews.com/claude-mythos-turning-n-days-into-n-hours-exploit/
Anthropic Released Claude Fable 5, the First Model in Mythos Class	https://cybersecuritynews.com/anthropic-claude-fable-5/

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
Researcher Hacked Google Using AI and Earned $500,000 Bug Bounty	https://cybersecuritynews.com/google-infrastructure-hacked-ai/
OpenClaw AI Agent Leaks Sensitive Credentials in New Phishing Attack Simulation	https://cybersecuritynews.com/openclaw-ai-agent-leaks-sensitive-credentials/

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
Microsoft Teams for Android Vulnerability Allows Attackers to Disclose Sensitive Data	https://cybersecuritynews.com/microsoft-teams-for-android-vulnerability/
Oracle PeopleSoft 0-Day RCE Vulnerability Exploited in Attacks by ShinyHunters	https://cybersecuritynews.com/oracle-peoplesoft-0-day-rce-vulnerability/
Microsoft Outlook and Word Vulnerabilities Allow Attackers to Execute Malicious Code	https://cybersecuritynews.com/microsoft-outlook-and-word-vulnerabilities/
Palo Alto PAN-OS Vulnerability Allows Attackers to Execute Arbitrary Commands as Root User	https://cybersecuritynews.com/palo-alto-pan-os-vulnerability/
Critical Langflow Vulnerability Exploited to Execute Malicious Code	https://cybersecuritynews.com/langflow-vulnerability-exploit/
CISA Warns of Check Point Security Gateway Vulnerability Actively Exploited in Ransomware Attacks	https://cybersecuritynews.com/cisa-check-point-security-gateway-vulnerability/
Ivanti Command Injection Vulnerability Exploited in Attacks Following PoC Release	https://cybersecuritynews.com/ivanti-command-injection-vulnerability-exploit/
PoC Exploit Released for Guest-to-Host Escape Linux Kernel Vulnerability	https://cybersecuritynews.com/poc-exploit-released-linux-kernel-vulnerability/
GreatXML BitLocker Bypass 0-Day Exploited Via Windows Defender Offline Scan	https://cybersecuritynews.com/greatxml-bitlocker-bypass-0-day-exploited/
Microsoft Exchange Server 0-Day Vulnerability Exploited in Attacks Using Weaponized Email	https://cybersecuritynews.com/microsoft-exchange-server-0-day-exploited/
Ivanti Endpoint Manager Mobile Vulnerability Enables Remote Code Execution Attacks	https://cybersecuritynews.com/ivanti-endpoint-manager-mobile-vulnerability/
Windows Collaborative Translation Framework 0-Day Vulnerability Allows Privilege Escalation	https://cybersecuritynews.com/windows-collaborative-framework-0-day-vulnerability/
CISA Warns of Google Chromium 0-Day Vulnerability Exploited in Attacks	https://cybersecuritynews.com/google-chromium-0-day-vulnerability-exploit/
Windows RDP Vulnerabilities Allow Attacker to Expose Sensitive Data	https://cybersecuritynews.com/windows-remote-desktop-protocol-vulnerabilities/
Critical OpenSSL Vulnerabilities Enable Remote Code Execution Attacks	https://cybersecuritynews.com/openssl-rce-vulnerability/

Windows BitLocker 0-Day Vulnerability Allows Attackers to Bypass Security Feature	https://cybersecuritynews.com/windows-bitlocker-0-day-bypass-vulnerability/
New Windows Defender 0-Day Exploit “RoguePlanet” Grants SYSTEM Access to Attackers	https://cybersecuritynews.com/windows-defender-0-day-exploit-rogueplanet/

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
Google Patches 28 Chrome Vulnerabilities that Allow Attackers to Execute Malicious Code	https://cybersecuritynews.com/28-chrome-vulnerabilities-patched/
Oracle Emergency Security Update to Fix Critical RCE Vulnerability	https://cybersecuritynews.com/oracle-security-update/

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
Hackers Use Free Spotify Premium Hacks on TikTok and Instagram to Spread Vidar Infostealer	https://cybersecuritynews.com/hackers-use-free-spotify-premium-hacks/
Solana FakeFix Campaign Uses 25 Malicious npm and PyPI Packages to Steal Developer Secrets	https://cybersecuritynews.com/solana-fakefix-campaign-uses-25-malicious-npm-and-pypi-packages/
GoFlateLoader Uses Massive PE Overlay to Deliver Lumma, Vidar, and StealC Infostealers	https://cybersecuritynews.com/goflateloader-uses-massive-pe-overlay/
Hackers Abuse SniperDz PhaaS Ecosystem for Brand Impersonation and Browser Hijacking	https://cybersecuritynews.com/hackers-abuse-sniperdz-phaas-ecosystem/
Hackers Use Weaponized DMG Files to Target macOS Users With Infostealer Malware	https://cybersecuritynews.com/hackers-use-weaponized-dmg-files/
Hackers Use BLUERABBIT Backdoor to Encrypt Files and Wipe Disks Across Windows Systems	https://cybersecuritynews.com/hackers-use-bluerabbit-backdoor/
Hackers Abuse Residential Proxy Networks to Hide Malicious Activity and Evade Detection	https://cybersecuritynews.com/hackers-abuse-residential-proxy-networks/
Hackers Abuse VMware-Signed Binary to Sideload NIGHTFORGE Loader in Espionage Attacks	https://cybersecuritynews.com/hackers-abuse-vmware-signed-binary-to-sideload-nightforge-loader/
Multiple Splunk Enterprise Vulnerabilities Allow Attackers to Execute Malicious Script	https://cybersecuritynews.com/multiple-splunk-enterprise-vulnerabilities/

Hackers Abuse AWS CloudTrail and Google Cloud Logging to Evade Detection and Exfiltrate Logs	https://cybersecuritynews.com/hackers-abuse-aws-cloudtrail-and-google-cloud-logging/
Anthropic's Claude Fable 5 Jailbroken to Generate Stack Exploits	https://cybersecuritynews.com/anthropics-claude-fable-5-jailbroken/
Hackers Abuse Fake Utility Downloads to Install ScreenConnect and Mine Cryptocurrency	https://cybersecuritynews.com/hackers-abuse-fake-utility-downloads/
Hackers Use Tax Phishing Emails to Deploy In-Memory Malware on Windows Systems	https://cybersecuritynews.com/hackers-use-tax-phishing-emails/
ServiceNow Confirms Vulnerability Allowing Unauthorized Access to Customer Instance Tables	https://cybersecuritynews.com/servicenow-confirms-vulnerability/
Hackers Infect npm Package dbmux With Malware to Fully Compromise Developer Systems	https://cybersecuritynews.com/hackers-infect-npm-package-dbmux-with-malware/
73 Microsoft Packages Weaponized to Deploy Password Stealer Malware	https://cybersecuritynews.com/73-microsoft-packages-weaponized/
Hackers Deploy MLTBackdoor Malware via Multi-Stage ClickFix Infection Chain	https://cybersecuritynews.com/hackers-deploy-mltbackdoor-malware/
Hackers Abuse TikTok and Instagram Reels to Spread Malware via Fake Free Software Tutorials	https://cybersecuritynews.com/hackers-abuse-tiktok-and-instagram-reels-to-spread-malware/
New MagicAd Android Malware Flood Device With Ads Bypassing Restrictions	https://cybersecuritynews.com/new-magicad-android-malware-flood-device/
New Browser-in-the-Browser Phishing Attack to Steal Microsoft 365 Logins	https://cybersecuritynews.com/new-browser-in-the-browser-phishing-attack/

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

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/