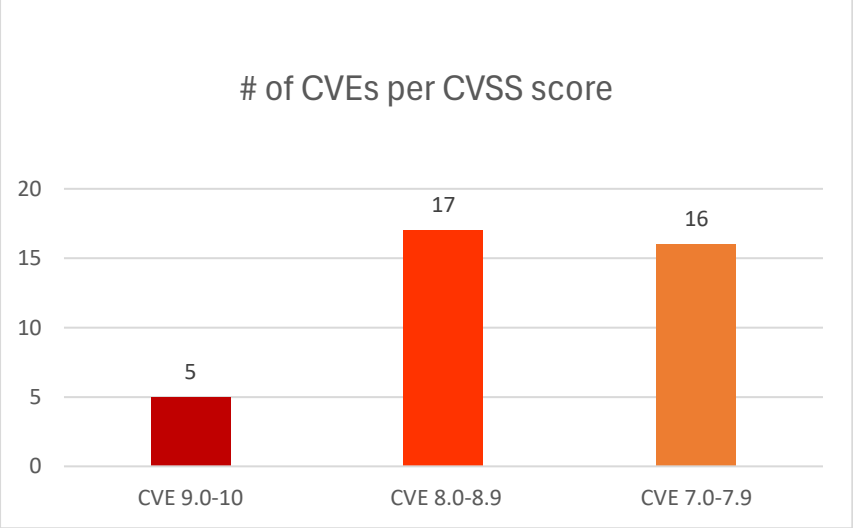
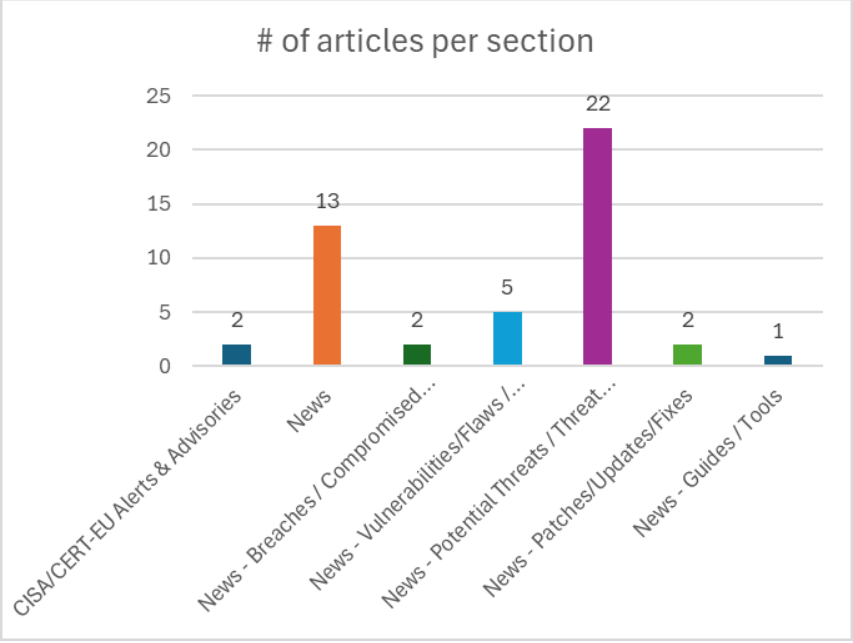
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 24/06/2026 - 26/06/2026





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-2026-52806	9,9	Gogs	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Gogs is an open source self-hosted Git service. Prior to 0.14.3	https://github.com/gogs/gogs/commit/a9dbafbfd8e1020bacc626420238c01d75d03364 https://github.com/gogs/gogs/pull/8301 https://github.com/gogs/gogs/releases/tag/v0.14.3 https://github.com/gogs/gogs/security/advisories/GHSA-qf6p-p7ww-cwr9
https://nvd.nist.gov/vuln/detail/CVE-2026-49980	9,8	Rclone	Missing Authentication for Critical Function	Rclone is a command-line program to sync files and directories to and from different cloud storage providers. From 1.46.0 until 1.74.3	https://github.com/rclone/rclone/security/advisories/GHSA-qw24-gh76-8rvv
https://nvd.nist.gov/vuln/detail/CVE-2026-57881	9,8	GeoVision	Stack-based Buffer Overflow	GeoVision GV-LPC2011 and GV-LPC2211 V1.12 and earlier	https://www.geovision.com.tw/cyber_security.php
https://nvd.nist.gov/vuln/detail/CVE-2026-53943	9,6	Ghost	Use of Cache Containing Sensitive Information	Ghost is a Node.js content management system. From until 6.37.0	https://github.com/TryGhost/Ghost/security/advisories/GHSA-62q6-4hv4-vjrw
https://nvd.nist.gov/vuln/detail/CVE-2026-56351	9,6	n8n	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	n8n before version 2.4.0 contains a sql injection vulnerability in MySQL, PostgreSQL, and Microsoft SQL nodes	https://github.com/n8n-io/n8n/security/advisories/GHSA-f3f2-mcxc-pwjx https://www.vulncheck.com/advisories/n8n-sql-injection-in-mysql-postgresql-and-microsoft-sql-nodes
https://nvd.nist.gov/vuln/detail/CVE-2026-13026	8,8	Google Chrome	Use After Free	Use after free in Digital Credentials in Google Chrome on Mac prior to 149.0.7827.197	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0482630350.html https://issues.chromium.org/issues/519728279
https://nvd.nist.gov/vuln/detail/CVE-2026-13027	8,8	Google Chrome	Use After Free	Use after free in FileSystem in Google Chrome prior to 149.0.7827.197	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0482630350.html https://issues.chromium.org/issues/520543781
https://nvd.nist.gov/vuln/detail/CVE-2026-13031	8,8	Google Chrome	Use After Free	Use after free in Blink in Google Chrome prior to 149.0.7827.197	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0482630350.html https://issues.chromium.org/issues/523308824
https://nvd.nist.gov/vuln/detail/CVE-2026-13033	8,8	Google Chrome	Out-of-bounds Read, Out-of-bounds Write	Out of bounds read and write in Blink>InterestGroups in Google Chrome prior to 149.0.7827.197	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0482630350.html https://issues.chromium.org/issues/523677844
https://nvd.nist.gov/vuln/detail/CVE-2026-13035	8,8	Google Chrome	Use After Free	Use after free in Bluetooth in Google Chrome on Mac prior to 149.0.7827.197	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0482630350.html https://issues.chromium.org/issues/523704570
https://nvd.nist.gov/vuln/detail/CVE-2026-13036	8,8	Google Chrome	Use After Free	Use after free in Blink in Google Chrome prior to 149.0.7827.197	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0482630350.html https://issues.chromium.org/issues/523711130

https://nvd.nist.gov/vuln/detail/CVE-2026-13038	**8,8**	Google Chrome	Use After Free	Google Chrome on Windows prior to 149.0.7827.197	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0482630350.html https://issues.chromium.org/issues/523740781
https://nvd.nist.gov/vuln/detail/CVE-2026-49247	**8,8**	Jellyfin	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Jellyfin is an open source self hosted media server. From 10.9.0 until 10.11.10	https://github.com/jellyfin/jellyfin/security/advisories/GHSA-jg92-mrxq-vv75
https://nvd.nist.gov/vuln/detail/CVE-2026-56766	**8,8**	Hydra	Stack-based Buffer Overflow	Hydra through 9.7	https://github.com/vanhauser-thc/thc-hydra/commit/9cc84c20e75f5fef6bb1790bb9ada2afad2204e2 https://www.vulncheck.com/advisories/hydra-stack-buffer-overflow-in-ntlm-authentication-handler
https://nvd.nist.gov/vuln/detail/CVE-2026-12053	**8,6**	GitLab	Insertion of Sensitive Information into Log File	GitLab EE affecting all versions from 19.1 before 19.1.1	https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-1-1-released/ https://gitlab.com/gitlab-org/gitlab/-/work_items/602194 https://hackerone.com/reports/3757762
https://nvd.nist.gov/vuln/detail/CVE-2026-47389	**8,6**	Mastodon	Incomplete List of Disallowed Inputs	Mastodon is a free, open-source social network server based on ActivityPub. Prior to 4.5.10, 4.4.17, and 4.3.23	https://github.com/mastodon/mastodon/security/advisories/GHSA-xx55-4rrg-8xg6
https://nvd.nist.gov/vuln/detail/CVE-2026-49269	**8,6**	Apple M1 GPUs	Exposure of Sensitive Information to an Unauthorized Actor	Apple M1 GPUs	https://gist.github.com/scndls/9cbe31f2b0b1578eaeb311e601335355
https://nvd.nist.gov/vuln/detail/CVE-2026-57877	**8,6**	GeoVision	Use of Externally-Controlled Format String	vlsvr in GeoVision GV-LPC2011 and GV-LPC2211 V1.12 and earlier	https://www.geovision.com.tw/cyber_security.php
https://nvd.nist.gov/vuln/detail/CVE-2026-13025	**8,3**	Google Chrome	Improper Input Validation	Race in DevTools in Google Chrome prior to 149.0.7827.197	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0482630350.html https://issues.chromium.org/issues/518043569
https://nvd.nist.gov/vuln/detail/CVE-2026-55762	**8,1**	Rocket.Chat	Missing Authorization	Prior to 8.5.1, 8.4.4, 8.3.6, 8.2.6, 8.1.6, 8.0.7, and 7.10.13	https://github.com/RocketChat/Rocket.Chat/security/advisories/GHSA-8hhc-j325-rxqp
https://nvd.nist.gov/vuln/detail/CVE-2026-9222	**8,1**	Setracker2 Android Companion App	Use of Password Hash Instead of Password for Authentication	Setracker2 Android Companion App com.tgelec.setracker versions 3.1.5 and prior	https://raw.githubusercontent.com/cisagov/CSAF/refs/heads/develop/csaf_files/VA/white/2026/va-26-176-01.json
https://nvd.nist.gov/vuln/detail/CVE-2026-23879	**8,0**	py7zr	Improper Link Resolution Before File Access ('Link Following')	py7zr is a Python-based library and utility to support 7zip archive compression, decompression, encryption and decryption. Versions 1.1.2 and below	https://github.com/miurahr/py7zr/releases/tag/v1.1.3 https://github.com/miurahr/py7zr/security/advisories/GHSA-q6rc-2cgv-63h7
https://nvd.nist.gov/vuln/detail/CVE-2026-13037	**7,8**	Google Chrome	Use After Free	Use after free in WebView in Google Chrome on Android prior to 149.0.7827.197	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0482630350.html https://issues.chromium.org/issues/523721871
https://nvd.nist.gov/vuln/detail/CVE-2026-46607	**7,8**	Glances	Deserialization of Untrusted Data	Glances is an open-source system cross-platform monitoring tool. Prior to 4.5.5	https://github.com/nicolargo/glances/releases/tag/v4.5.5 https://github.com/nicolargo/glances/security/advisories/GHSA-9837-48hr-q32j
https://nvd.nist.gov/vuln/detail/CVE-2026-46735	**7,8**	Dell Display and Peripheral Manager (DDPM Mac)	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Dell Display and Peripheral Manager (DDPM Mac), versions prior to 2.3	https://www.dell.com/support/kbdoc/en-hk/000475656/dsa-2026-267?msockid=3021cac2195069ed3194ddad186a68f9

https://nvd.nist.gov/vuln/detail/CVE-2026-48731	**7,8**	Warp	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Warp is an agentic development environment. From 0.2024.02.20.08.01.stable_01 until 0.2026.05.06.15.42.stable_01	https://github.com/warpdotdev/warp/commit/861dacea2683f2fe263c3c3a1381c3cbb2b66809 https://github.com/warpdotdev/warp/security/advisories/GHSA-7xgc-mhc8-g7wc
https://nvd.nist.gov/vuln/detail/CVE-2026-57456	**7,8**	Vim	Improper Control of Generation of Code ('Code Injection')	Vim is an open source, command line text editor. Prior to 9.2.0699	https://github.com/vim/vim/commit/cce141c42740f122dd8486ae04e21c2a81016ba8 https://github.com/vim/vim/releases/tag/v9.2.0699 https://github.com/vim/vim/security/advisories/GHSA-ppj8-wqjf-6fp3
https://nvd.nist.gov/vuln/detail/CVE-2026-54033	**7,7**	LibreChat	Server-Side Request Forgery (SSRF)	Prior to 0.8.4-rc1	https://github.com/danny-avila/LibreChat/security/advisories/GHSA-gc9r-88c3-7qhq
https://nvd.nist.gov/vuln/detail/CVE-2026-9099	**7,7**	Keycloak	Authorization Bypass Through User-Controlled Key	-	https://access.redhat.com/errata/RHSA-2026:30049 https://access.redhat.com/errata/RHSA-2026:30050 https://access.redhat.com/errata/RHSA-2026:30083 https://access.redhat.com/errata/RHSA-2026:30084 https://access.redhat.com/security/cve/CVE-2026-9099 https://bugzilla.redhat.com/show_bug.cgi?id=2480182
https://nvd.nist.gov/vuln/detail/CVE-2026-13029	**7,5**	Google Chrome	Use After Free	Use after free in Web Authentication in Google Chrome prior to 149.0.7827.197	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0482630350.html https://issues.chromium.org/issues/521495992
https://nvd.nist.gov/vuln/detail/CVE-2026-56122	**7,5**	Winstone Servlet Engine	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Winstone Servlet Engine through 0.9.10	https://gist.github.com/VAMorales/ce93f10215c43b2a8344426f4dd59cd3 https://winstone.sourceforge.net/ https://www.vulncheck.com/advisories/winstone-servlet-engine-path-traversal-via-http-request-paths
https://nvd.nist.gov/vuln/detail/CVE-2026-57589	**7,4**	OpenBSD	Use After Free	sys/kern/sysv_sem.c in OpenBSD through 7.9	https://github.com/openbsd/src/commit/1957873d2063db11dab780eca75b5e629d1e838d https://openai.com/index/patch-the-planet/
https://nvd.nist.gov/vuln/detail/CVE-2026-49506	**7,2**	Dell Wyse Management Suite	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Dell Wyse Management Suite, versions prior to WMS 5.5 HF1	https://www.dell.com/support/kbdoc/en-in/000465356/dsa-2026-225?msockid=3021cac2195069ed3194ddad186a68f9
https://nvd.nist.gov/vuln/detail/CVE-2026-47150	**7,1**	EmberZNet	Out-of-bounds Write	EmberZNet v9.0.2 and earlier	https://github.com/SiliconLabsSoftware/sisdk-release/ https://siliconlabs.lightning.force.com/sfc/servlet.shepherd/document/download/069Vm00000pEGPQIA4?operationContext=S1
https://nvd.nist.gov/vuln/detail/CVE-2026-56071	**7,1**	Forminator	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Forminator <= 1.53.1 versions	https://patchstack.com/database/wordpress/plugin/forminator/vulnerability/wordpress-forminator-plugin-1-53-1-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-56256	**7,1**	Capgo	Client-Side Enforcement of Server-Side Security	Capgo before 12.128.2	https://github.com/Cap-go/capgo/security/advisories/GHSA-cww4-5xfp-jw98 https://www.vulncheck.com/advisories/capgo-two-factor-authentication-bypass-via-organization-management-api
https://nvd.nist.gov/vuln/detail/CVE-2026-57303	**7,1**	Jenkins Assembla Plugin	Server-Side Request Forgery (SSRF)	Jenkins Assembla Plugin 1.4 and earlier	https://www.jenkins.io/security/advisory/2026-06-24/#SECURITY-3692%20(1)
https://nvd.nist.gov/vuln/detail/CVE-2026-57520	**7,1**	Bitwarden	Missing Authorization	Bitwarden Server before 2026.5.0	https://github.com/bitwarden/server/commit/901bb67157c0f80d369c40b76742fdf7623da4e4 https://github.com/bitwarden/server/pull/7526

					https://github.com/bitwarden/server/releases/tag/v2026.5.0 https://sanjokkarki.com.np/blog/bitwarden-bulk-remove-admin https://www.vulncheck.com/advisories/bitwarden-server-privilege-escalation-via-bulk-user-remove-endpoint

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-2026-12569 PTC Windchill and FlexPLM Improper Input Validation Vulnerability ▪ CVE-2026-20230 Cisco Unified Communications Manager Server-Side Request Forgery (SSRF) Vulnerability	https://www.cisa.gov/news-events/alerts/2026/06/25/cisa-adds-two-known-exploited-vulnerabilities-catalog
Using SASE in a Modern TIC 3.0 Solution		https://www.cisa.gov/resources-tools/resources/using-sase-modern-tic-30-solution

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
Microsoft Extends Windows 10 Security Updates for Users Up to October 2027	https://cybersecuritynews.com/microsoft-extends-windows-10-security-updates/
OpenAI Reportedly Delays ChatGPT 5.6 Release Following Trump Administration Request	https://cybersecuritynews.com/openai-delays-chatgpt-5-6-release/
Russia Used Cellebrite Tool to Hack Activist's iPhone Despite Contract Cancellation	https://cybersecuritynews.com/russia-cellebrite-tool-iphone/
Windows Secure Boot Certificate Expired — Billions of PCs Affected Including Linux Distros	https://cybersecuritynews.com/windows-secure-boot-certificate-expired/
Gemini 3.5 Flash Released With Computer Use Capabilities that Build Agents	https://cybersecuritynews.com/gemini-3-5-flash-released/
WhatsApp to Warn Users Before Starting Chats With New Phone Numbers	https://cybersecuritynews.com/whatsapp-warning-screen/
OpenClaw Skill Marketplace Exposes AI Agents to Supply Chain Malware and Financial Fraud	https://cybersecuritynews.com/openclaw-skill-marketplace-exposes-ai-agents/
Anthropic Accuses Alibaba of 'Illicitly' Accessing Its Claude AI Models in Largest Known Distillation Attack	https://cybersecuritynews.com/anthropic-accuses-alibaba/
Authorities Disrupt Stealer Malware StealC and Amadey Infrastructure in Global Operation	https://cybersecuritynews.com/stealc-infrastructure-disrupted/
GhostShell Malware Uses mTLS Implant and Telegram Dead-Drop to Target Ukrainian Drone Operations	https://cybersecuritynews.com/ghostshell-malware-uses-mtls-implant-and-telegram-dead-drop/
Claude Fable 5 Wrote Windows Kernel Code in Rust in 38 Minutes	https://cybersecuritynews.com/claude-fable-5-windows-kernel-code/
In-Browser Data Inspection Lets Analysts Track Phishing Attack Flow Inside Browser Sessions	https://cybersecuritynews.com/in-browser-data-inspection-lets-analysts-track-phishing-attack-flow/
Anthropic Launches Claude Tag – AI Teammate Now Lives Inside Slack	https://cybersecuritynews.com/anthropic-claude-tag/

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
Laravel Livewire Applications Compromised to Steal Credentials Exploiting RCE Vulnerability	https://cybersecuritynews.com/laravel-livewire-app-exploiting-rce-flaw/
Malicious AI Agent Skill Bypasses Security Scans and Seizes Full Control of Over 26,000 Agents	https://cybersecuritynews.com/malicious-ai-agent-skill-bypasses/

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
CISA Warns of Cisco Unified CM Vulnerability Exploited in Attacks	https://cybersecuritynews.com/cisco-unified-cm-vulnerability-2/
Hackers Exploiting Cisco Catalyst SD-WAN Manager 0-Day Flaw to Gain Root-Level Access	https://cybersecuritynews.com/cisco-catalyst-sd-wan-manager-0-day/
PoC Exploit Released for Microsoft Exchange Server Elevation of Privilege Vulnerability	https://cybersecuritynews.com/poc-exploit-released-exchange-vulnerability/
PoC Exploit Released for libssh2 Remote Code Execution Vulnerability	https://cybersecuritynews.com/poc-exploit-libssh2-rce-vulnerability/
CISA Warns of Ubiquiti UniFi OS Vulnerability Actively Exploited in Attacks	https://cybersecuritynews.com/cisa-ubiquiti-unifi-os-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
25-Year-Old Vulnerability in cURL Used by 30 Billion Devices Finally Patched	https://cybersecuritynews.com/25-year-old-curl-vulnerability/
Chrome 149 Security Update — Patch for Critical Flaws that Enable Code Execution Attacks	https://cybersecuritynews.com/chrome-149-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. Περι-λαμβάνονται αναφορές σε εργαλεία που χρησιμοποιούν οι επιτιθέμενοι, αλλά και δείκτες (IoCs) που μπορούν να χρησιμοποιηθούν στην άμυνα.

Σύντομη περιγραφή / Τίτλος	URL
Miasma Malware Uses binding.gyp and Bun to Execute Hidden Payloads in npm Packages	https://cybersecuritynews.com/miasma-malware-uses-binding-gyp-and-bun/
Minecraft Malware Loader Uses RSA-Signed Smart Contract Updates for Persistent C2	https://cybersecuritynews.com/minecraft-malware-loader-uses-rsa-signed/
LokiBot Campaign Uses JScript Attachment, .NET Injector, and Process Injection to Steal Credentials	https://cybersecuritynews.com/lokibot-campaign-uses-jscript-attachment/
Shai-Hulud Payload Steals GitHub, npm, Cloud, CI/CD, and SSH Credentials From De-velopers	https://cybersecuritynews.com/shai-hulud-payload-steals-github-npm-cloud/
AiTM Phishing Kits Steal Console Credentials and MFA Codes from AWS Environ-ments	https://cybersecuritynews.com/aitm-phishing-kit-steals-console-credentials/
Rust macOS Backdoor Uses Interactive Shell and Telegram File Uploads for Data Theft	https://cybersecuritynews.com/rust-macos-backdoor-uses-interactive-shell/
ManageEngine AD360 Integration Flaw Exposes User Identity and Role Information to Attackers	https://cybersecuritynews.com/manageengine-ad360-integration-flaw/
Malicious Chrome Extension Uses Native Messaging Host to Execute PowerShell Commands	https://cybersecuritynews.com/malicious-chrome-extension-uses-native-messaging-host/
Hackers Use Cisco AnyConnect and Google Update Lures to Drop SharkLoader Mal-ware	https://cybersecuritynews.com/hackers-use-cisco-anyconnect-and-google-update-lures/
Mistic Backdoor Blends With Microsoft Endpoint Security Tooling to Evade Detec-tion	https://cybersecuritynews.com/mistic-backdoor-blends-with-microsoft-endpoint-security/
Microsoft Teams Impersonation Campaign Enables Unauthorized Access Through RMM Abuse	https://cybersecuritynews.com/microsoft-teams-impersonation-campaign-enables-unauthorized-access/
Fake Document Reader in The Google Play Store with 100K Downloads Deliver An-droid Malware	https://cybersecuritynews.com/fake-document-reader-in-the-google-play-store/
Malicious Edge Extension Uses Chrome Native Messaging to Execute Code on Victim Systems	https://cybersecuritynews.com/malicious-edge-extension-uses-chrome-native-messaging/
EvilTokens Hides Its Attack Flow in the Browser, Exposing Static Analysis Gaps	https://cybersecuritynews.com/eviltokens-hides-its-attack-flow-in-the-browser/
Critical Webmin Vulnerabilities Allow Attackers to Impersonate as Any User	https://cybersecuritynews.com/webmin-vulnerabilities-impersonate-user/
Browser-in-the-Browser Kit Uses Fake Software Errors to Deliver Malware Installers	https://cybersecuritynews.com/browser-in-the-browser-kit-uses-fake-software-errors/
Red-Team AI Tool Vulnerabilities Let Attackers Exfiltrate API Keys and Compromise Operators' Systems	https://cybersecuritynews.com/red-team-ai-tool-vulnerabilities/
Hackers Exploit Unpatched SharePoint Servers to Deploy Ransomware and Custom Backdoors	https://cybersecuritynews.com/hackers-exploit-unpatched-sharepoint-servers/
GTA 6 Scam Websites Use AI-Generated Images and Fake Download Buttons to Lure Gamers	https://cybersecuritynews.com/gta-6-scam-websites-use-ai-generated-images/
FortiBleed Attack Hit 430,000+ FortiGate Firewalls, Stealing 110M+ Credentials	https://cybersecuritynews.com/fortibleed-attack-fortigate-firewalls/

Critical Cisco Unified CM and SME Flaw Enables Remote Attacker to Launch SSRF Attacks	https://cybersecuritynews.com/cisco-unified-cm-and-sme-flaw-ssrf-attacks/
Hackers Use GoogleErrorReport Scheduled Task for Persistence in Dropping Elephant Campaign	https://cybersecuritynews.com/hackers-use-googleerrorreport-scheduled-task-for-persistence/

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
How Attackers Exploit Privileged Access and How to Lock Them Out	https://cybersecuritynews.com/how-attackers-exploit-privileged-access/

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/