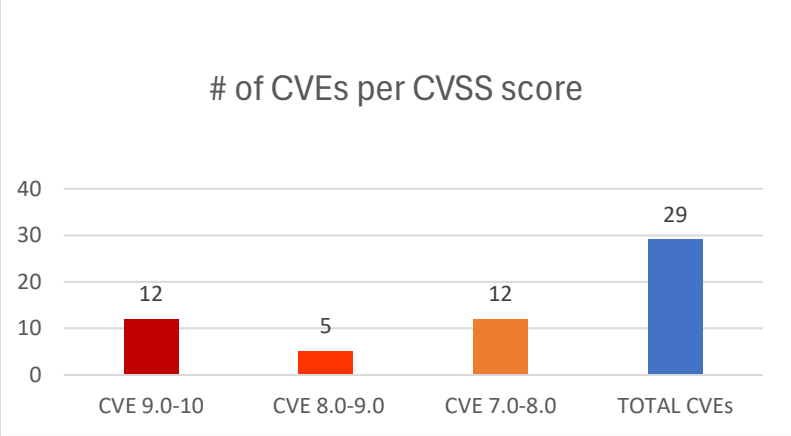
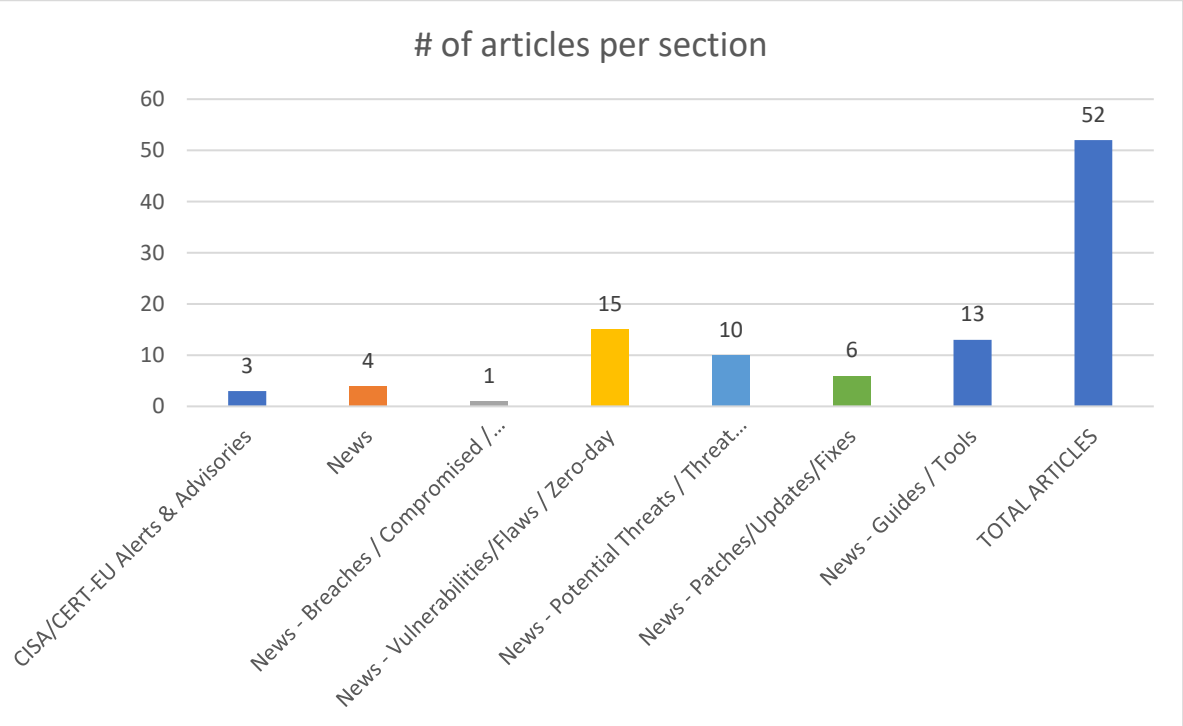
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 15/07/2026 - 17/07/2026





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 όπως 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-2026-45336	**10,0**	HireFlow	Use of Hard-coded Credentials	In 1.2 and earlier	https://github.com/StratonWebDesigners/HireFlow/releases/tag/v1.3 GitHub, Inc. https://github.com/StratonWebDesigners/HireFlow/security/advisories/GHSA-x53g-jr84-jrv5
https://nvd.nist.gov/vuln/detail/CVE-2026-50148	**10,0**	Metabase	External Control of File Name or Path	From 1.54.0 until 1.54.24, 1.55.24, 1.56.25, 1.57.19, 1.58.14, 1.59.10, and 1.60.4	https://github.com/metabase/metabase/security/advisories/GHSA-r6x2-rchx-q9g9
https://nvd.nist.gov/vuln/detail/CVE-2026-46512	**9,9**	Frogman	Improper Control of Generation of Code ('Code Injection')	Prior to 1.6.2	https://github.com/mwtcmi/frogman/commit/36a05ffa2df1d256b6f6f7c3b66ef77ebe3e458a GitHub, Inc. https://github.com/mwtcmi/frogman/releases/tag/v1.6.1 GitHub, Inc. https://github.com/mwtcmi/frogman/releases/tag/v1.6.2 GitHub, Inc. https://github.com/mwtcmi/frogman/security/advisories/GHSA-pxfc-q72v-jh8m
https://nvd.nist.gov/vuln/detail/CVE-2026-53412	**9,8**	Zoom Desktop Client for Windows	Improper Input Validation		https://www.zoom.com/en/trust/security-bulletin/zsb-26014
https://nvd.nist.gov/vuln/detail/CVE-2026-63087	**9,8**	Grafana OnCall	Missing Authentication for Critical Function	through 1.16.11	https://github.com/geo-chen/oss/blob/main/oncall.md VulnCheck https://www.vulncheck.com/advisories/grafana-oncall-unauthenticated-token-hijack-via-plugin-install-endpoint
https://nvd.nist.gov/vuln/detail/CVE-2026-44180	**9,8**	Jupyter Enterprise Gateway	Improper Input Validation	Versions 2.0.0rc1 and above prior to 3.3.0	https://github.com/jupyter-server/enterprise_gateway/releases/tag/v3.3.0 GitHub, Inc. https://github.com/jupyter-server/enterprise_gateway/security/advisories/GHSA-chq7-94j8-cj28

https://nvd.nist.gov/vuln/detail/CVE-2026-30623	**9,8**	LiteLLM	Improper Neutralization of Special Elements used in a Command ('Command Injection')	1.18.10	https://docs.litellm.ai/blog/mcp-stdio-command-injection-april-2026 MITRE https://github.com/BerriAI/litellm MITRE https://www.ox.security/blog/mcp-supply-chain-advisory-rce-vulnerabilities-across-the-ai-ecosystem/
https://nvd.nist.gov/vuln/detail/CVE-2025-65720	**9,8**	Open Source GPT Researcher	Improper Neutralization of Special Elements used in a Command ('Command Injection')	v3.3.7	https://github.com/assafelovic/gpt-researcher MITRE https://www.ox.security/blog/gpt-researcher-remote-code-execution MITRE https://www.ox.security/blog/mcp-supply-chain-advisory-rce-vulnerabilities-across-the-ai-ecosystem/
https://nvd.nist.gov/vuln/detail/CVE-2026-56400	**9,6**	open-webui	Insufficient Session Expiration	before 0.3.14	https://github.com/open-webui/open-webui/security/advisories/GHSA-6xcp-7mpr-m7wm CISA-ADP, VulnCheck Vendor Advisory https://www.vulncheck.com/advisories/open-webui-remote-code-execution-via-cors-misconfiguration-and-session-validation
https://nvd.nist.gov/vuln/detail/CVE-2026-62948	**9,6**	OpenWrt	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Prior to 25.12.5	https://github.com/openwrt/luci/commit/55379d04fcc3c605003a5001d6135cf02ae6048a GitHub, Inc. https://github.com/openwrt/odhcpd/commit/68f382690bfaec56d5b1f31c3c31c48bcb642e3a GitHub, Inc. https://github.com/openwrt/odhcpd/pull/404 GitHub, Inc. https://github.com/openwrt/openwrt/releases/tag/v25.12.5 GitHub, Inc. https://github.com/openwrt/openwrt/security/advisories/GHSA-hhmc-92hw-535f
https://nvd.nist.gov/vuln/detail/CVE-2026-63089	**9,3**	WireGuard Easy	Insufficient Session Expiration	through 15.3.0	https://github.com/wg-easy/wg-easy/commit/66b292b11bde3664f05ffb016c8082665d261ded VulnCheck https://github.com/wg-easy/wg-easy/pull/2661 VulnCheck https://www.vulncheck.com/advisories/wireguard-easy-weak-token-generation-information-disclosure-via-otl-route
https://nvd.nist.gov/vuln/detail/CVE-2026-62241	**9,1**	clawvet self-hosted API server (apps/api)	Missing Authentication for Critical Function	before 0.7.5	https://github.com/MohibShaikh/clawvet/security/advisories/GHSA-9mww-p953-jfc9 VulnCheck https://www.vulncheck.com/advisories/clawvet-hard-coded-jwt-secret-session-forgery
https://nvd.nist.gov/vuln/detail/CVE-2026-62228	**8,8**	OpenClaw	Incorrect Authorization	before 2026.6.5	https://github.com/openclaw/openclaw/security/advisories/GHSA-8f46-3xx3-8c9m VulnCheck https://www.vulncheck.com/advisories/openclaw-authorization-bypass-via-node-exec-approvals

https://nvd.nist.gov/vuln/detail/CVE-2026-49998	**8,2**	Centrifugo	Improper Verification of Cryptographic Signature	Prior to 6.8.1	https://github.com/centrifugal/centrifugo/commit/15d785015c6f318c1b68ea40b813699c9f8bd2c4 GitHub, Inc. https://github.com/centrifugal/centrifugo/pull/1142 GitHub, Inc. https://github.com/centrifugal/centrifugo/releases/tag/v6.8.1 GitHub, Inc. https://github.com/centrifugal/centrifugo/security/advisories/GHSA-g6vg-wj8f-48cj
https://nvd.nist.gov/vuln/detail/CVE-2026-57821	**8,1**	Apache Fineract's Office Search API	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to and including 1.14.0	https://github.com/apache/fineract/pull/6048 Apache Software Foundation Patch https://lists.apache.org/thread/lb7zwdv7qntzy6z05gzf7m8mxw9cbgsj Apache Software Foundation Mailing List Vendor Advisory https://lists.apache.org/thread/rj5vwh3z2xcvsf0rqwj8kokpbrxkhq4n
https://nvd.nist.gov/vuln/detail/CVE-2026-55173	**8,1**	WWBN Avideo	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Versions 29.0	https://github.com/WWBN/AVideo/commit/c1cfa2bea8a351a1d07f5758f82887403e3abf1f GitHub, Inc. https://github.com/WWBN/AVideo/security/advisories/GHSA-wc3f-xc32-435f
https://nvd.nist.gov/vuln/detail/CVE-2026-46353	**8,1**	BigBlueButton	Improper Access Control	Prior to 3.0.21	https://github.com/bigbluebutton/bigbluebutton/commit/36fd1b407488a0c56ce620b91184d5a8aea68b3d GitHub, Inc. https://github.com/bigbluebutton/bigbluebutton/releases/tag/v3.0.21 GitHub, Inc. https://github.com/bigbluebutton/bigbluebutton/security/advisories/GHSA-43hc-5g2m-cqff
https://nvd.nist.gov/vuln/detail/CVE-2026-53411	**7,8**	Zoom Clients for Windows	Improper Input Validation		https://www.zoom.com/en/trust/security-bulletin/zsb-26013
https://nvd.nist.gov/vuln/detail/CVE-2026-40952	**7,8**	Secure Access installer for the Windows client	Insufficient Information	prior to version 14.55	https://www.absolute.com/platform/security-information/vulnerability-archive/cve-2026-40952
https://nvd.nist.gov/vuln/detail/CVE-2026-62309	**7,5**	CoreDNS	NULL Pointer Dereference	Prior to 1.14.4	https://github.com/coredns/coredns/commit/60a439dd4febfcd78e3779e952fe3fbf3c16bb1f GitHub, Inc. https://github.com/coredns/coredns/pull/8154 GitHub, Inc. https://github.com/coredns/coredns/releases/tag/v1.14.4 GitHub, Inc. https://github.com/coredns/coredns/security/advisories/GHSA-9rvv-m5g5-wc8r

https://nvd.nist.gov/vuln/detail/CVE-2026-44453	**7,5**	h2o	Memory Allocation with Excessive Size Value		https://github.com/h2o/h2o/commit/6b5370d9d09fcf83aa7620ddf77de1954a192181 GitHub, Inc. https://github.com/h2o/h2o/security/advisories/GHSA-rf9v-m59p-mq84
https://nvd.nist.gov/vuln/detail/CVE-2026-44436	**7,5**	Quicly	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')		https://github.com/h2o/quicly/commit/8b178e692c51a3b1031612ef89f03a53aac63c15 GitHub, Inc. https://github.com/h2o/quicly/security/advisories/GHSA-v55w-59qx-2v78
https://nvd.nist.gov/vuln/detail/CVE-2026-39359	**7,5**	Wazuh	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	In versions 4.0.0 through 4.10.3 and 4.11.0 through 4.14.4	https://github.com/wazuh/wazuh/security/advisories/GHSA-6q95-fcwc-4h44
https://nvd.nist.gov/vuln/detail/CVE-2026-36590	**7,5**	EMQ NanoMQ	Missing Release of Resource after Effective Lifetime	v.0.24.9	https://github.com/MoXie25/NanoMQ-Memory-Leak-Research.git MITRE Vendor Advisory https://github.com/MoXie25/NanoMQ-Memory-Leak-Research/blob/main/README.md
https://nvd.nist.gov/vuln/detail/CVE-2026-38755	**7,5**	the evalcommand() function (shell/ash.c) of Busybox	Heap-based Buffer Overflow	v1.38.0	https://busybox.com MITRE Product https://lists.busybox.net/pipermail/busybox/2026-June/092354.html
https://nvd.nist.gov/vuln/detail/CVE-2026-62290	**7,3**	cert-manager	Incorrect Authorization	From 1.18.0 until 1.19.6 and 1.20.3	https://github.com/cert-manager/cert-manager/commit/6bda47297c8fbc6b121b8b76624b668d26f1a155 GitHub, Inc. https://github.com/cert-manager/cert-manager/commit/b37dbf01ecea50a0b3a19df0a7fe4c5ad6803f16 GitHub, Inc. https://github.com/cert-manager/cert-manager/pull/8940 GitHub, Inc. https://github.com/cert-manager/cert-manager/pull/8941 GitHub, Inc. https://github.com/cert-manager/cert-manager/releases/tag/v1.19.6 GitHub, Inc. https://github.com/cert-manager/cert-manager/releases/tag/v1.20.3 GitHub, Inc. https://github.com/cert-manager/cert-manager/security/advisories/GHSA-8rvj-mm4h-c258
https://nvd.nist.gov/vuln/detail/CVE-2026-62387	**7,1**	The Grav API plugin	Permissive Cross-domain Policy with Untrusted Domains	before 1.0.0-rc.16	https://github.com/getgrav/grav/security/advisories/GHSA-93px-98wh-6fj2 VulnCheck https://www.vulncheck.com/advisories/grav-rc-16-cors-misconfiguration-via-api-plugin

https://nvd.nist.gov/vuln/detail/CVE-2026-46336	**7,1**	Manyfold	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	From 0.96.0 until 0.140.0	https://github.com/manyfold3d/manyfold/commit/ed6a53e54926708594c07d222155ac3a22f93174 GitHub, Inc. https://github.com/manyfold3d/manyfold/pull/6122 GitHub, Inc. https://github.com/manyfold3d/manyfold/releases/tag/v0.140.0 GitHub, Inc. https://github.com/manyfold3d/manyfold/security/advisories/GHSA-j5f9-r7wf-hv37
https://nvd.nist.gov/vuln/detail/CVE-2026-61389	**7,0**	Productivity Suite	Out-of-bounds Write		https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-197-04.json ICS-CERT https://www.automationdirect.com/support/software-downloads ICS-CERT https://www.cisa.gov/news-events/ics-advisories/icsa-26-197-04

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-2023-4346 KNX Association KNX Protocol Connection Authorization Option 1 Overly Restrictive Account Lockout Mechanism Vulnerability ▪ CVE-2026-46817 Oracle E-Business Suite Improper Privilege Management Vulnerability	https://www.cisa.gov/news-events/alerts/2026/07/15/cisa-adds-two-known-exploited-vulnerabilities-catalog
Establishing a Coordinated Vulnerability Disclosure Program to Work With Security Researchers		https://www.cisa.gov/resources-tools/resources/establishing-coordinated-vulnerability-disclosure-program-work-security-researchers
CISA Adds Three Known Exploited Vulnerabilities to Catalog	▪ CVE-2026-25089 Fortinet FortiSandbox OS Command Injection Vulnerability ▪ CVE-2026-39808 Fortinet FortiSandbox OS Command Injection Vulnerability ▪ CVE-2026-58644 Microsoft SharePoint Deserialization of Untrusted Data Vulnerability	https://www.cisa.gov/news-events/alerts/2026/07/16/cisa-adds-three-known-exploited-vulnerabilities-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
Government Updates UK's National Risk Register with Cyber Warnings	https://www.infosecurity-magazine.com/news/uk-national-risk-register-cyber/
Chinese Hackers Embed Claude Code and DeepSeek in AI-Powered Government Cyberattacks	https://cybersecuritynews.com/chinese-hackers-ai-attacks/
Police Disrupt a €140M Cyber Fraud Ring in Spain	https://www.darkreading.com/threat-intelligence/police-disrupt-140m-euro-cyber-fraud-ring-spain
GPT-5.6 Codex is Reportedly Deleting Files From Home Directories	https://cybersecuritynews.com/gpt-5-6-codex-delete-files/

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
Two Hackers Jailed for Hacking 148 TfL Systems, Forcing Password Reset for 27,000 Staff	https://cybersecuritynews.com/two-scattered-spider-hackers-jailed/

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
Windows BitLocker 0-Day Vulnerability Allows Hackers to Bypass Security Feature	https://cybersecuritynews.com/windows-bitlocker-0-day-vulnerability-2/
Multiple Notepad++ Vulnerabilities Enable PowerShell Command Injection Attacks	https://cybersecuritynews.com/notepad-vulnerabilities-command-injection/
Microsoft Active Directory Services 0-Day Vulnerability Actively Exploited in the Wild	https://cybersecuritynews.com/active-directory-services-0-day-exploited/
New LegacyHive Windows 0-day Vulnerability Allows Users to Load Another User's Registry	https://cybersecuritynews.com/legacyhive-windows-0-day-vulnerability/

Critical Cursor 0-Day Flaw Allows Malicious Git Repos to Trigger Automatic Windows Code Execution	https://cybersecuritynews.com/critical-cursor-0-day-flaw/
Multiple Dell PowerProtect Vulnerabilities Allow Hackers to Gain Full System Access Remotely	https://cybersecuritynews.com/multiple-dell-powerprotect-vulnerabilites/
Multiple Windows RDP Vulnerabilities Allow Attackers to Access Sensitive Data	https://cybersecuritynews.com/windows-remote-desktop-protocol-vulnerabilities-2/
Two SonicWall SMA 1000 Zero-Days Exploited, One Could Enable Admin Commands	https://thehackernews.com/2026/07/two-sonicwall-sma-1000-zero-days.html
Cursor Flaw Lets Malicious Cloned Repositories Trigger Windows Code Execution	https://thehackernews.com/2026/07/cursor-flaw-lets-malicious-cloned.html
Researcher Drops New Windows Zero-Day PoC Hours After Microsoft Patch Tuesday	https://thehackernews.com/2026/07/researcher-drops-new-windows-zero-day.html
Zoom warns of critical account takeover vulnerability	https://www.bleepingcomputer.com/news/security/zoom-warns-of-critical-account-takeover-vulnerability/
Progress Confirms Zero-Day Vulnerability Behind ShareFile Disruption	https://www.securityweek.com/progress-confirms-zero-day-vulnerability-behind-sharefile-disruption/
Nightmare Eclipse Drops 'LegacyHive' Windows Zero-Day	https://www.securityweek.com/nightmare-eclipse-drops-legacyhive-windows-zero-day/
7-Zip Vulnerability Exposes Millions of Users to Remote Code Execution Risk	https://cybersecuritynews.com/7-zip-vulnerability-code-execution/
CISA Warns of Fortinet FortiSandbox OS Injection Vulnerabilities Exploited in Attacks	https://cybersecuritynews.com/fortisandbox-vulnerabilities-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 Patches 570 CVEs in Record Patch Tuesday	https://www.infosecurity-magazine.com/news/microsoft-570-cves-patch-tuesday/
F5 Patches Multiple NGINX Vulnerabilities Enabling Heap Buffer Overflow and Code Execution Attacks	https://cybersecuritynews.com/f5-patches-multiple-nginx-vulnerabilities/
Chrome 150 Security Update Patches 15 Flaws, Including Two Critical Code Execution Ones	https://cybersecuritynews.com/chrome-150-security-update/
Firefox, Chrome, Adobe, and VMware Updates Fix Multiple Critical Security Flaws	https://thehackernews.com/2026/07/firefox-chrome-adobe-and-vmware-updates.html
Vulnerabilities Patched by Fortinet, Ivanti, ServiceNow	https://www.securityweek.com/vulnerabilities-patched-by-fortinet-ivanti-servicenow/
JetBrains Patched 6 Vulnerabilities Across TeamCity, YouTrack and IntelliJ IDEA	https://cybersecuritynews.com/jetbrains-patched-vulnerabilities/

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
Phishing Campaign Abuses eCards to Deploy RMM Tools	https://www.infosecurity-magazine.com/news/seasonalinvite-phishing-ecards-rmm/
Compromised Logins Surge as the Most Common Entry Point for Ransomware At-tacks	https://www.infosecurity-magazine.com/news/compromised-logins-ransomware-entry/
Hackers Abuse Shared Claude Chats and Google Ads to Deploy MacSync Stealer on macOS	https://cybersecuritynews.com/shared-claude-chats-macsync-stealer/
Hackers Abuse FaceTime Calls to Impersonate Banks and Hijack Victims' Accounts	https://cybersecuritynews.com/facetime-calls-impersonate-banks/
CISA Warns of Microsoft SharePoint Server Vulnerability Actively Exploited in At-tacks	https://cybersecuritynews.com/sharepoint-server-vulnerability-exploited/
New Rust-Based LabubaRAT Impersonates NVIDIA Software to Hijack Windows Systems	https://cybersecuritynews.com/labubarat-nvidia-malware/
Critical SonicWall Firewall 0-Day Vulnerabilities Actively Exploited in Attacks	https://cybersecuritynews.com/sonicwall-firewall-0-day-vulnerabilities-exploited/
Gamers Download Fake Cheats and Hand Attackers a Live Remote Control of Their Windows PCs	https://cybersecuritynews.com/game-fake-cheats-remote-access/
Claude Flaw Automatically Sends Malicious Prompts to AI Agents	https://www.darkreading.com/vulnerabilities-threats/claude-flaw-malicious-prompts-ai-agents
WhatsApp GhostPairing Lets Scammers Hijack Accounts Without Stealing Pass-words	https://cybersecuritynews.com/whatsapp-ghostpairing-hijack-accounts/

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
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
Top 10 Best Malware Sandbox Tools for Security Teams in 2026	https://cybersecuritynews.com/best-malware-sandbox-tools/
Top 5 Best Tools for Simulated DDoS Attacks in 2026	https://cybersecuritynews.com/simulated-ddos-attacks/

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/