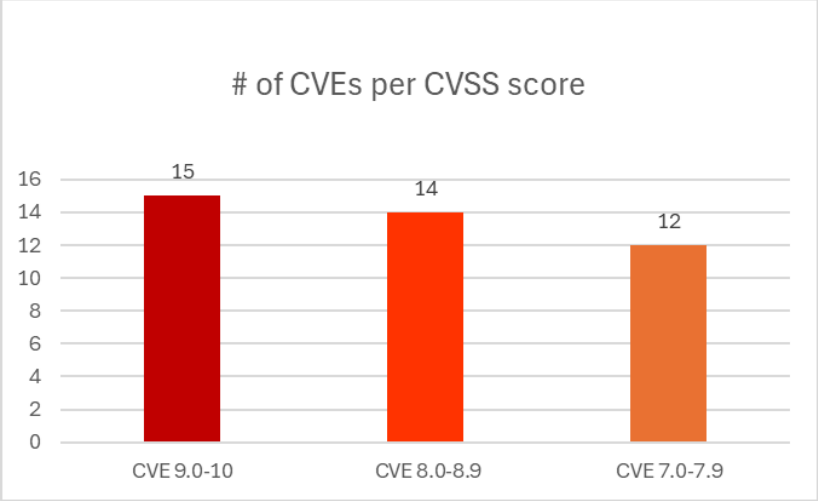
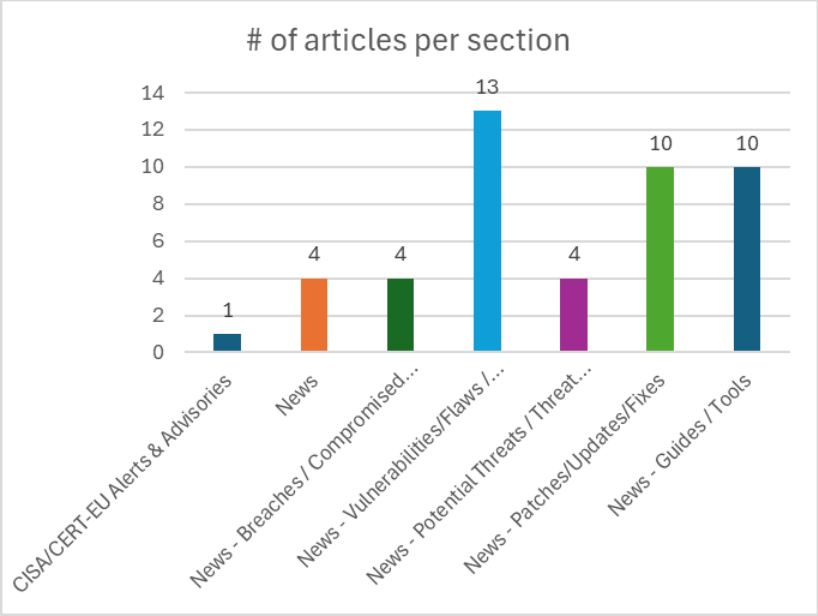
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 11/03/2026 - 13/03/2026





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)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2026-31957	10,0	Himmelblau is an interoperability suite for Microsoft Azure Entra ID and Intune	Insecure Default Initialization of Resource	From 3.0.0 to before 3.1.0	https://github.com/himmelblau-idm/himmelblau/security/advisories/GHSA-q746-m2wv-qh4v
https://nvd.nist.gov/vuln/detail/CVE-2026-3611	10,0	Honeywell IQ4x	Missing Authentication for Critical Function		https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-069-03.json https://www.cisa.gov/news-events/ics-advisories/icsa-26-069-03 https://www.honeywell.com/us/en/contact
https://nvd.nist.gov/vuln/detail/CVE-2025-66956	9,9	Asseco SEE	Improper Access Control	Contact Plan, E-Mail, SMS and Fax components in Asseco SEE Live 2.0	http://asseco.com http://live.com https://github.com/TheWoodenBench/CVE-2025-66956
https://nvd.nist.gov/vuln/detail/CVE-2026-21666	9,9	Veeam	Improper Access Control		https://www.veeam.com/kb4830
https://nvd.nist.gov/vuln/detail/CVE-2019-25468	9,8	NetGain	Improper Control of Generation of Code ('Code Injection')	NetGain EM Plus 10.1.68	http://netgain-systems.com https://www.exploit-db.com/exploits/47391 https://www.vulncheck.com/advisories/netgain-em-plus-remote-code-execution-via-script-test-jsp
https://nvd.nist.gov/vuln/detail/CVE-2025-67038	9,8	Lantronix EDS5000	Improper Control of Generation of Code ('Code Injection')	Lantronix EDS5000 2.1.0.0R3	http://eds5000.com http://lantronix.com https://www.cisa.gov/news-events/ics-advisories/icsa-26-069-02
https://nvd.nist.gov/vuln/detail/CVE-2025-70082	9,8	Lantronix EDS3000PS	Improper Neutralization of Special Elements used in an OS Command ('OS	Lantronix EDS3000PS v.3.1.0.0R2	http://eds3000ps.com http://lantronix.com https://www.cisa.gov/news-events/ics-advisories/icsa-26-069-02

			Command Injection')		
https://nvd.nist.gov/vuln/detail/CVE-2026-23813	9,8	AOS-CX switches	Improper Authentication		https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05027en_us&docLocale=en_US
https://nvd.nist.gov/vuln/detail/CVE-2026-26793	9,8	GL-iNet GL-AR300M16	Improper Neutralization of Special Elements used in a Command ('Command Injection')	GL-iNet GL-AR300M16 v4.3.11	https://github.com/sezangel/IOT-vul/tree/main/GL-iNet/GL-AR300M16/set_config
https://nvd.nist.gov/vuln/detail/CVE-2026-30903	9,8	Mail feature of Zoom Workplace for Windows	External Control of File Name or Path	Mail feature of Zoom Workplace for Windows before 6.6.0	https://www.zoom.com/en/trust/security-bulletin/zsb-26005
https://nvd.nist.gov/vuln/detail/CVE-2026-32136	9,8	AdGuard	Improper Authentication	Prior to 0.107.73	https://github.com/AdguardTeam/AdGuardHome/security/advisories/GHSA-5fg6-wrq4-w5gh
https://nvd.nist.gov/vuln/detail/CVE-2026-3916	9,6	Google Chrome	Out-of-bounds Read	Google Chrome prior to 146.0.7680.71	https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html https://issues.chromium.org/issues/482828615
https://nvd.nist.gov/vuln/detail/CVE-2026-32096	9,3	Plunk	Server-Side Request Forgery (SSRF)	Prior to 0.7.0	https://github.com/useplunk/plunk/commit/b8f1ad9ab53c78f8ef063fdc125f397c8bfc7652 https://github.com/useplunk/plunk/security/advisories/GHSA-xpqg-p8mp-7g44
https://nvd.nist.gov/vuln/detail/CVE-2026-31862	9,1	Cloud CLI (aka Claude Code UI)	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Prior to 1.24.0	https://github.com/siteboon/claudecodeui/releases/tag/v1.24.0 https://github.com/siteboon/claudecodeui/security/advisories/GHSA-f2fc-vc88-6w7q
https://nvd.nist.gov/vuln/detail/CVE-2023-27573	9,0	netbox-docker	Use of Default Credentials	netbox-docker before 2.5.0	https://github.com/netbox-community/netbox-docker/issues/953 https://github.com/netbox-community/netbox-docker/pull/959 https://github.com/netbox-community/netbox-docker/releases/tag/2.5.0
https://nvd.nist.gov/vuln/detail/CVE-2023-43010	8,8	Apple		The issue was addressed with improved memory handling. This issue is fixed in iOS 17.2 and iPadOS 17.2, macOS Sonoma 14.2, Safari 17.2, iOS 16.7.15 and iPadOS 16.7.15, iOS 15.8.7 and iPadOS 15.8.7	https://support.apple.com/en-us/120300 https://support.apple.com/en-us/120877 https://support.apple.com/en-us/120879 https://support.apple.com/en-us/126632 https://support.apple.com/en-us/126646

https://nvd.nist.gov/vuln/detail/CVE-2025-68623	8,8	Microsoft DirectX	Improper Access Control	Microsoft DirectX End-User Runtime Web Installer 9.29.1974.0	https://talosintelligence.com/vulnerability_reports/TALOS-2025-2293 https://www.microsoft.com/en-us/download/details.aspx?id=35 https://www.talosintelligence.com/vulnerability_reports/TALOS-2025-2293
https://nvd.nist.gov/vuln/detail/CVE-2026-3920	8,8	WebML in Google Chrome	Out-of-bounds Read	in WebML in Google Chrome prior to 146.0.7680.71	https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html https://issues.chromium.org/issues/482875307
https://nvd.nist.gov/vuln/detail/CVE-2026-3926	8,8	V8 in Google Chrome	Out-of-bounds Read	in V8 in Google Chrome prior to 146.0.7680.71	https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html https://issues.chromium.org/issues/478659010
https://nvd.nist.gov/vuln/detail/CVE-2026-3931	8,8	Google Chrome	Heap-based Buffer Overflow	in Skia in Google Chrome prior to 146.0.7680.71	https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html https://issues.chromium.org/issues/417599694
https://nvd.nist.gov/vuln/detail/CVE-2026-3936	8,8	Google Chrome on Android	Use After Free	Google Chrome on Android prior to 146.0.7680.71	https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html https://issues.chromium.org/issues/481920229
https://nvd.nist.gov/vuln/detail/CVE-2026-3971	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda i3 1.0.0.6(2204)	https://github.com/Svigo-o/Tenda_vul/tree/main/tenda-i3-formwrlSSIDset-go-buffer-overflow https://github.com/Svigo-o/Tenda_vul/tree/main/tenda-i3-formwrlSSIDset-index-buffer-overflow https://vuldb.com/?ctiid.350406 https://vuldb.com/?id.350406 https://vuldb.com/?submit.768996 https://vuldb.com/?submit.768997 https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-3978	8,8	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	D-Link DIR-513 1.10	https://github.com/Litengzheng/vul_db/blob/main/Dir513/vul_21/README.md https://vuldb.com/?ctiid.350413 https://vuldb.com/?id.350413 https://vuldb.com/?submit.769586 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-4008	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda W3 1.0.0.3(2204)	https://github.com/Svigo-o/Tenda_vul/tree/main/tenda-w3-formwrlSSIDset-go-buffer-overflow https://github.com/Svigo-o/Tenda_vul/tree/main/tenda-w3-formwrlSSIDset-index-buffer-overflow https://vuldb.com/?ctiid.350531 https://vuldb.com/?id.350531 https://vuldb.com/?submit.769182 https://vuldb.com/?submit.769183 https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-4043	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda i12 1.0.0.6(2204)	https://github.com/Jimi-Lab/cve/issues/3 https://vuldb.com/?ctiid.350655 https://vuldb.com/?id.350655 https://vuldb.com/?submit.769464 https://www.tenda.com.cn/

https://nvd.nist.gov/vuln/detail/CVE-2026-1090	8,7	GitLab	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	in GitLab CE/EE affecting all versions from 10.6 before 18.7.6, 18.8 before 18.8.6, and 18.9 before 18.9.2	https://about.gitlab.com/releases/2026/03/11/patch-release-gitlab-18-9-2-released/ https://gitlab.com/gitlab-org/gitlab/-/work_items/586478 https://hackerone.com/reports/3502450
https://nvd.nist.gov/vuln/detail/CVE-2019-25483	8,4	Comtrend	Missing Authentication for Critical Function	Comtrend AR-5310 GE31-412SSG-C01_R10.A2pG039u.d24k	https://www.exploit-db.com/exploits/47149 https://www.vulncheck.com/advisories/comtrend-ar-5310-ge31-412ssg-c01-r10-a2pg039u-d24k-restricted-shell-escape
https://nvd.nist.gov/vuln/detail/CVE-2026-32138	8,2	NEXULEAN	Improper Access Control	NEXULEAN is a cybersecurity portfolio & service platform for an Ethical Hacker, AI Enthusiast, and Penetration Tester. Prior to 2.0.0	https://github.com/Stalin-143/website/releases/tag/v2.0.0 https://github.com/Stalin-143/website/security/advisories/GHSA-r7cr-5wcx-x9wm
https://nvd.nist.gov/vuln/detail/CVE-2026-25529	8,1	Postal	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Postal versions less than 3.3.5	https://github.com/postalserver/postal/security/advisories/GHSA-5f4r-5jpr-rfhc
https://nvd.nist.gov/vuln/detail/CVE-2026-30902	7,8	Zoom	Improper Privilege Management	in certain Zoom Clients for Windows	https://www.zoom.com/en/trust/security-bulletin/zsb-26004
https://nvd.nist.gov/vuln/detail/CVE-2026-21887	7,7	OpenCTI	Server-Side Request Forgery (SSRF)	Prior to 6.8.16	https://github.com/OpenCTI-Platform/opencti/security/advisories/GHSA-ffm6-vvph-g5f5
https://nvd.nist.gov/vuln/detail/CVE-2026-32117	7,6	Grafana	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	0.1.2 and earlier	https://github.com/ekacnet/grafanacubism-panel/commit/b79cbf7e5eb3225bb204bcef274e15e6b19d9926 https://github.com/ekacnet/grafanacubism-panel/security/advisories/GHSA-q6fh-6m3m-5948
https://nvd.nist.gov/vuln/detail/CVE-2019-25470	7,5	eWON	Use of Hard-coded Credentials	eWON Firmware versions 12.2 to 13.0	https://www.ewon.biz https://www.exploit-db.com/exploits/47380 https://www.vulncheck.com/advisories/ewon-firmware-authentication-bypass-via-wsdreadform
https://nvd.nist.gov/vuln/detail/CVE-2019-25472	7,5	IntelBras	External Control of File Name or Path	IntelBras Telefone IP TIP200 and 200 LITE	https://backend.intelbras.com/sites/default/files/integration/lamina_tip-200-lite_e_tip-200.pdf https://www.exploit-db.com/exploits/47337 https://www.vulncheck.com/advisories/intelbras-telefone-ip-tip200-200-lite-arbitrary-file-read-via-dumpconfigfile

https://nvd.nist.gov/vuln/detail/CVE-2026-28356	7,5	multipart is a fast multi-part/form-data parser for python	Inefficient Regular Expression Complexity	multipart is a fast multi-part/form-data parser for python. Prior to 1.2.2, 1.3.1 and 1.4.0-dev	https://github.com/defnull/multipart/security/advisories/GHSA-p2m9-wcp5-6qw3
https://nvd.nist.gov/vuln/detail/CVE-2026-20074	7,4	Cisco IOS XR Software	Improper Validation of Specified Type of Input		https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-isis-dos-kDMxpSzK
https://nvd.nist.gov/vuln/detail/CVE-2026-3943	7,3	H3C	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	H3C ACG1000-AK230 up to 20260227	https://github.com/leeyper/CVE/issues/1 https://vuldb.com/?ctiid.350353 https://vuldb.com/?id.350353 https://vuldb.com/?submit.768850
https://nvd.nist.gov/vuln/detail/CVE-2026-20163	7,2	Splunk	Improper Neutralization of Special Elements used in a Command ('Command Injection')	In Splunk Enterprise versions below 10.2.0, 10.0.4, 9.4.9, and 9.3.10, and Splunk Cloud Platform versions below 10.2.2510.5, 10.0.2503.12, 10.1.2507.16, and 9.3.2411.124	https://advisory.splunk.com/advisories/SVD-2026-0302
https://nvd.nist.gov/vuln/detail/CVE-2026-23816	7,2	AOS-CX Switches	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')		https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05027en_us&docLocale=en_US
https://nvd.nist.gov/vuln/detail/CVE-2026-2368	7,1	Lenovo Filez application	Improper Certificate Validation		https://www.filez.com/securityPolicy
https://nvd.nist.gov/vuln/detail/CVE-2026-30901	7,0	Zoom	Improper Input Validation	in Zoom Rooms for Windows before 6.6.5 in Kiosk Mode	https://www.zoom.com/en/trust/security-bulletin/zsb-26003

CISA/CERT-EU Alerts & Advisories

Αυτό το κομμάτι περιλαμβάνει ειδοποιήσεις από επίσημες πηγές, κυρίως CISA και CERT-EU, σχετικά με κρίσιμες ευπάθειες ή ενεργές απειλές. Συνήθως αφορούν βιομηχανικά ή κρίσιμα συστήματα, αλλά και mainstream λογισμικό. Προσφέρονται σε μορφή σύντομων αναφορών και οδηγούν σε πιο λεπτομερείς τεχνικές οδηγίες.

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2025-68613 n8n Improper Control of Dynamically-Managed Code Resources Vulnerability	https://www.cisa.gov/news-events/alerts/2026/03/11/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
Iran MOIS Colludes With Criminals to Boost Cyberattacks	https://www.darkreading.com/threat-intelligence/iran-mois-criminals-cyberattacks
Cyber-Attacks on UK Firms Increase at Four Times Global Rate	https://www.infosecurity-magazine.com/news/cyberattacks-uk-firms-increase/
Researchers Discover Major Security Gaps in LLM Guardrails	https://www.infosecurity-magazine.com/news/major-security-gaps-llm-guardrails/
France: National Cybersecurity Agency Reports Ransomware Attack Drop in 2025	https://www.infosecurity-magazine.com/news/france-anssi-ransomware-attack/

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
Bell Ambulance data breach impacted over 238,000 people	https://securityaffairs.com/189343/data-breach/bell-ambulance-data-breach-impacted-over-238000-people.html?&web_view=true
Ally WordPress Plugin Flaw Exposes Over 200,000 Websites to Attacks	https://www.securityweek.com/ally-wordpress-plugin-flaw-exposes-over-200000-websites-to-attacks/
Xygeni GitHub Action Compromised Via Tag Poison	https://www.darkreading.com/application-security/xygeni-github-action-compromised-via-tag-poison
Ericsson US Discloses Data Breach – Hackers Stolen Employees and Customers Data	https://cybersecuritynews.com/ericsson-data-breach/

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 Flags Actively Exploited n8n RCE Bug as 24,700 Instances Remain Exposed	https://thehackernews.com/2026/03/cisa-flags-actively-exploited-n8n-rce.html
Critical n8n Flaws Allow Remote Code Execution and Exposure of Stored Credentials	https://thehackernews.com/2026/03/critical-n8n-flaws-allow-remote-code.html
Critical N8n Vulnerabilities Allowed Server Takeover	https://www.securityweek.com/critical-n8n-vulnerabilities-allowed-server-takeover/
SQLi flaw in Elementor Ally plugin impacts 250k+ WordPress sites	https://www.bleepingcomputer.com/news/security/sqli-flaw-in-elementor-ally-plugin-impacts-250k-plus-wordpress-sites/
Researchers Uncover 'LeakyLooker' Vulnerabilities in Google Looker Studio	https://www.infosecurity-magazine.com/news/google-looker-studios-security-gaps/
Critical CrackArmor Vulnerabilities Expose 12.6 Million Linux Servers to Complete Root Takeover	https://cybersecuritynews.com/crackarmor-vulnerability/
OpenSSH GSSAPI Vulnerability Allow an Attacker to Crash SSH Child Processes	https://cybersecuritynews.com/openssh-gssapi-vulnerability/
Critical MediaTek Vulnerability Lets Attackers Steal Android Phone PINs in 45 Seconds	https://cybersecuritynews.com/mediatek-vulnerability-android-phone/
Microsoft Copilot Email and Teams Summarization Vulnerability Enables Phishing Attacks	https://cybersecuritynews.com/microsoft-copilot-summarization-vulnerability/
Paloalto Cortex XDR Broker Vulnerability Attackers to Obtain and Modify Sensitive Information	https://cybersecuritynews.com/paloalto-cortex-xdr-broker-vulnerability/
Splunk RCE Vulnerability Allows Attackers to Execute Arbitrary Shell Commands	https://cybersecuritynews.com/splunk-rce-vulnerability-2/
SolarWinds Web Help Desk Deserialization Vulnerability Enables Command Execution	https://cybersecuritynews.com/solarwinds-web-help-desk-deserialization-vulnerability/
Critical Microsoft Office Vulnerability Enables Remote Code Execution Attacks	https://cybersecuritynews.com/microsoft-office-vulnerability-enables-rce-attack/

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
Veeam Patches 7 Critical Backup & Replication Flaws Allowing Remote Code Execution	https://thehackernews.com/2026/03/veeam-patches-7-critical-backup.html
Apple Issues Security Updates for Older iOS Devices Targeted by Coruna WebKit Exploit	https://thehackernews.com/2026/03/apple-issues-security-updates-for-older.html
Dozens of Vendors Patch Security Flaws Across Enterprise Software and Network Devices	https://thehackernews.com/2026/03/dozens-of-vendors-patch-security-flaws.html
Microsoft Patches 84 Flaws in March Patch Tuesday, Including Two Public Zero-Days	https://thehackernews.com/2026/03/microsoft-patches-84-flaws-in-march.html
Splunk, Zoom Patch Severe Vulnerabilities	https://www.securityweek.com/splunk-zoom-patch-severe-vulnerabilities/
Cisco Patches High-Severity IOS XR Vulnerabilities	https://www.securityweek.com/cisco-patches-high-severity-ios-xr-vulnerabilities-2/
Fortinet, Ivanti, Intel Patch High-Severity Vulnerabilities	https://www.securityweek.com/fortinet-ivanti-intel-patch-high-severity-vulnerabilities/
Microsoft Fixes Two Publicly Disclosed Zero-Days	https://www.infosecurity-magazine.com/news/microsoft-fixes-two-publicly/
GitLab Security Update – Patch for XSS and API DoS Vulnerabilities	https://cybersecuritynews.com/gitlab-security-update-2/
Chrome Security Update – Patch for 29 Vulnerabilities that Allow Remote Code Execution	https://cybersecuritynews.com/chrome-security-update-29-vulnerabilities/

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
Compromised WordPress Sites Deliver ClickFix Attacks in Global Infostealer Campaign	https://www.infosecurity-magazine.com/news/wordpress-clickfix-infostealer/
PixRevolution Malware Hijacks Brazil's PIX Transfers in Real Time	https://www.infosecurity-magazine.com/news/pixrevolution-malware-brazils-pix/
Attackers Hijack Microsoft 365 Accounts Through OAuth Device Code Abuse Without Stealing Passwords	https://cybersecuritynews.com/oauth-device-code-phishing-attack/
Hackers Leveraging Cloudflare Anti-Bot Features to Steal Microsoft 365 Credentials	https://cybersecuritynews.com/cloudflare-anti-bot-features-microsoft-365/

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
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

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/