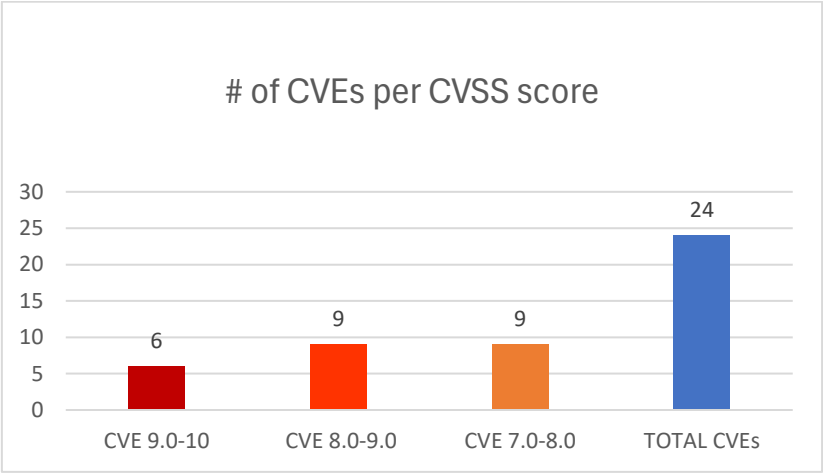
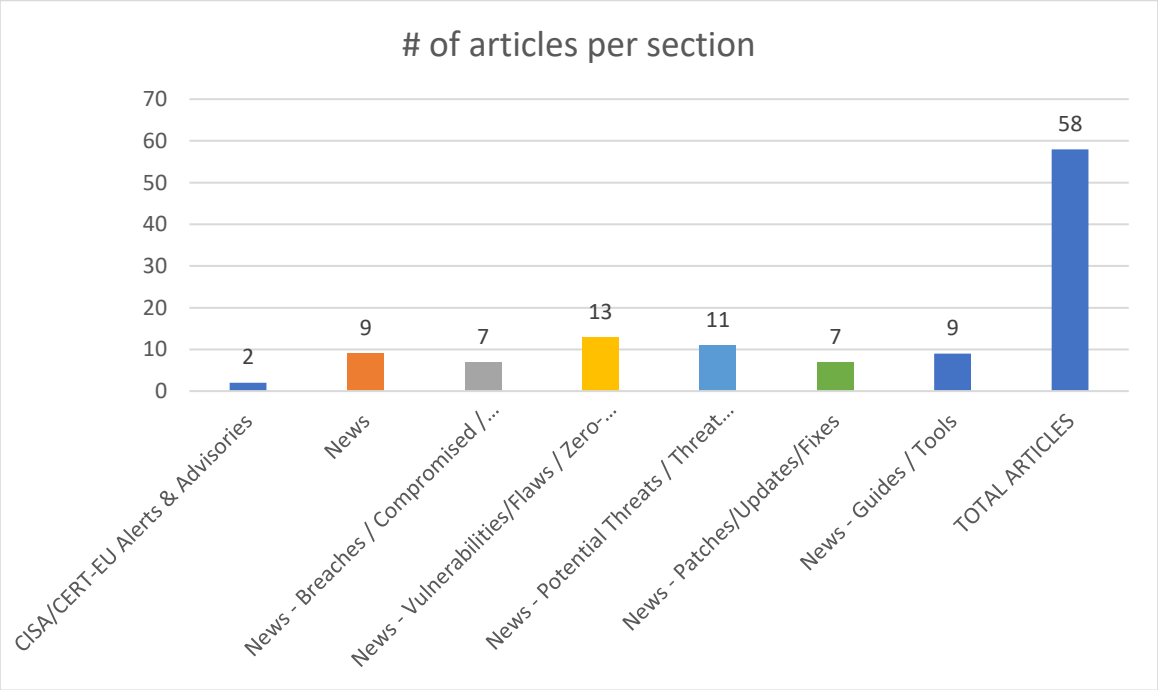
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 25/02/2026 - 27/02/2026





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-2026-3301	9,8	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	N300RH 6.1c.1353_B20190305	https://github.com/xyh4ck/iot_poc/blob/main/TOTOLINK/N300RHv4/01_setWebWlanIdx_RCE/README.md VulDB https://vuldb.com/?ctiid.348052 VulDB https://vuldb.com/?id.348052 VulDB https://vuldb.com/?submit.761297 VulDB https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-3164	9,8	News Portal Project	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	1.0	https://github.com/a936848435/cve-report-cyy/issues/1 VulDB Exploit Third Party Advisory https://itsourcecode.com/ VulDB Product https://vuldb.com/?ctiid.347671 VulDB Permissions Required VDB Entry https://vuldb.com/?id.347671 VulDB Third Party Advisory VDB Entry https://vuldb.com/?submit.759546
https://nvd.nist.gov/vuln/detail/CVE-2026-3152	9,8	College Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/ltranquility/cve_submit/issues/6 VulDB Exploit Third Party Advisory https://itsourcecode.com/ VulDB Product https://vuldb.com/?ctiid.347660 VulDB Permissions Required VDB Entry https://vuldb.com/?id.347660 VulDB Third Party Advisory VDB Entry https://vuldb.com/?submit.758834
https://nvd.nist.gov/vuln/detail/CVE-2026-3148	9,8	Source-Codester Simple and	Improper Neutralization of Special Elements used in an	1.0	https://github.com/xiaoxiaojie12/CVE/issues/1 VulDB Exploit Third Party Advisory https://vuldb.com/?ctiid.347654 VulDB Permissions Required VDB Entry

		Nice Shopping Cart Script	SQL Command ('SQL Injection')		https://vuldb.com/?id.347654 VulDB Third Party Advisory VDB Entry https://vuldb.com/?submit.758822 VulDB Third Party Advisory VDB Entry https://www.sourcecodester.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-28213	9,8	EverShop	Weak Password Recovery Mechanism for Forgotten Password	prior to 2.1.1	https://github.com/evershopcommerce/evershop/releases/tag/v2.1.1 GitHub, Inc. https://github.com/evershopcommerce/evershop/security/advisories/GHSA-cg73-g723-39jw
https://nvd.nist.gov/vuln/detail/CVE-2026-28370	9,1	OpenStack Vitrage	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	before 12.0.1, 13.0.0, 14.0.0, and 15.0.0	https://github.com/openstack/vitrage/blob/a1f86950e1314b0c740f9cd9b7e9dbab7d02af51/vitrage/graph/query.py#L70 MITRE https://storyboard.openstack.org/#%21/story/2011539
https://nvd.nist.gov/vuln/detail/CVE-2026-3275	8,8	Tenda	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	F453 1.0.0.3	https://github.com/Litengzheng/vul_db/blob/main/F453/vul_75/README.md VulDB https://vuldb.com/?ctiid.347999 VulDB https://vuldb.com/?id.347999 VulDB https://vuldb.com/?submit.759622 VulDB https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-49113	8,8	Roundcube Webmail	Deserialization of Untrusted Data	before 1.5.10 and 1.6.x before 1.6.11	http://www.openwall.com/lists/oss-security/2025/06/02/3 CVE Mailing List Third Party Advisory https://fearsoff.org/research/roundcube MITRE Third Party Advisory https://github.com/roundcube/roundcubemail/commit/0376f69e958a8fef7f6f09e352c541b4e7729c4d MITRE Patch https://github.com/roundcube/roundcubemail/commit/7408f31379666124a39f9cb1018f62bc5e2dc695 MITRE Patch https://github.com/roundcube/roundcubemail/commit/c50a07d88ca38f018a0f4a0b008e9a1deb32637e MITRE Patch https://github.com/roundcube/roundcubemail/pull/9865 MITRE Issue Tracking

					https://github.com/roundcube/roundcubemail/releases/tag/1.5.10 MITRE Release Notes https://github.com/roundcube/roundcubemail/releases/tag/1.6.11 MITRE Release Notes https://lists.debian.org/debian-lts-announce/2025/06/msg00008.html CVE Mailing List Third Party Advisory https://roundcube.net/news/2025/06/01/security-updates-1.6.11-and-1.5.10 MITRE Vendor Advisory https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2025-49113 CISA-ADP US Government Resource https://www.vicarius.io/vsociety/posts/cve-2025-49113-roundcube-mitigation-script MITRE Exploit Mitigation Third Party Advisory https://www.vicarius.io/vsociety/posts/cve-2025-49113-roundcube-vulnerability-detection
https://nvd.nist.gov/vuln/detail/CVE-2026-27976	8,8	Zed	UNIX Symbolic Link (Symlink) Following	Prior to version 0.224.4	https://github.com/zed-industries/zed/security/advisories/GHSA-59p4-3mhm-qm3r
https://nvd.nist.gov/vuln/detail/CVE-2026-3071	8,4	the LanguageModel class of Flair	Deserialization of Untrusted Data	from versions 0.4.1 to latest	https://www.hiddenlayer.com/sai-security-advisory/2026-02-flair
https://nvd.nist.gov/vuln/detail/CVE-2026-28216	8,3	hoppscotch	Authorization Bypass Through User-Controlled Key	Prior to version 2026.2.0	https://github.com/hoppscotch/hoppscotch/releases/tag/2026.2.0 GitHub, Inc. https://github.com/hoppscotch/hoppscotch/security/advisories/GHSA-72rv-vc3j-5vqr
https://nvd.nist.gov/vuln/detail/CVE-2026-3179	8,1	The FTP Backup on the ADM	Improper Limitation of a Pathname	from ADM 4.1.0 through ADM 4.3.3.ROF1 as	https://www.asustor.com/security/security_advisory_detail?id=53

			to a Restricted Directory ('Path Traversal')	well as from ADM 5.0.0 through ADM 5.1.2.RE51	
https://nvd.nist.gov/vuln/detail/CVE-2026-3172	8,1	HNSW index build in pgvector	Out-of-bounds Write	0.6.0 through 0.8.1	https://github.com/pgvector/pgvector/issues/959
https://nvd.nist.gov/vuln/detail/CVE-2026-28275	8,1	Initiative	Insufficient Session Expiration	prior to 0.32.4	https://github.com/Morelitea/initiative/releases/tag/v0.32.4 GitHub, Inc. https://github.com/Morelitea/initiative/security/advisories/GHSA-hww6-3fww-xw3h
https://nvd.nist.gov/vuln/detail/CVE-2026-3037	8,0	XWEB Pro	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	1.12.1 and prior	https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-057-10.json ICS-CERT https://webapps.copeland.com/Dixell/Pages/SystemSoftwareUpdate ICS-CERT https://www.cisa.gov/news-events/ics-advisories/icsa-26-057-10
https://nvd.nist.gov/vuln/detail/CVE-2026-28364	7,9	OCaml	Buffer Over-read	before 4.14.3 and 5.x before 5.4.1	https://github.com/ocaml/security-advisories/blob/generated-osv/2026/OSEC-2026-01.json MITRE https://osv.dev/vulnerability/OSEC-2026-01
https://nvd.nist.gov/vuln/detail/CVE-2026-28211	7,8	The NVDA Dev & Test Toolbox	Improper Neutralization of Special Elements in Data Query Logic	2.0 through 8.0	https://github.com/CyrilleB79/NVDA-Dev-Test-Toolbox/commit/21a0544432b08971b5d18320e8256be12c610bea GitHub, Inc. https://github.com/CyrilleB79/NVDA-Dev-Test-Toolbox/releases/tag/V9.0 GitHub, Inc. https://github.com/CyrilleB79/NVDA-Dev-Test-Toolbox/security/advisories/GHSA-39pg-6xpm-mjgf

https://nvd.nist.gov/vuln/detail/CVE-2026-28136	7,6	VeronaLabs WP SMS wp-sms	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	from n/a through <= 6.9.12	https://patchstack.com/database/Wordpress/Plugin/wp-sms/vulnerability/wordpress-wp-sms-plugin-6-9-12-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-28372	7,4	telnetd in GNU inetutils	Inclusion of Functionality from Untrusted Control Sphere	through 2.7	https://git.hadrons.org/cgit/debian/pkgs/inetutils.git/commit/?id=3953943d8296310485f98963883a798545ab9a6c MITRE https://lists.gnu.org/archive/html/bug-inetutils/2026-02/msg00000.html MITRE https://lists.gnu.org/archive/html/bug-inetutils/2026-02/msg00012.html MITRE https://www.openwall.com/lists/oss-security/2026/02/24/1
https://nvd.nist.gov/vuln/detail/CVE-2026-3261	7,3	School Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/Ning-BJ/cve/issues/1 VulDB https://itsourcecode.com/ VulDB https://vuldb.com/?ctiid.347984 VulDB https://vuldb.com/?id.347984 VulDB https://vuldb.com/?submit.749364
https://nvd.nist.gov/vuln/detail/CVE-2026-3200	7,3	z-9527 admin	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0/2.0	https://github.com/CC-T-454455/Vulnerabilities/tree/master/z9527-admin/vulnerability-1 VulDB https://github.com/CC-T-454455/Vulnerabilities/tree/master/z9527-admin/vulnerability-2 VulDB https://vuldb.com/?ctiid.347772 VulDB https://vuldb.com/?id.347772 VulDB https://vuldb.com/?submit.758325 VulDB https://vuldb.com/?submit.758326 VulDB https://vuldb.com/?submit.758327 VulDB https://vuldb.com/?submit.758328 VulDB https://vuldb.com/?submit.758330
https://nvd.nist.gov/vuln/detail/CVE-2026-28279	7,3	osctrl is an osquery	Improper Neutralization of Special Elements used in an OS	Prior to version 0.5.0	https://github.com/jmpsec/osctrl/pull/777 GitHub, Inc. https://github.com/jmpsec/osctrl/pull/780 GitHub, Inc. https://github.com/jmpsec/osctrl/security/advisories/GHSA-rchw-322g-f7rm

		manage-ment solu-tion	Command ('OS Com-mand Injection')		
https://nvd.nist.gov/vuln/de-tail/CVE-2026-28138	7,2	Stylemix uListing	Deserialization of Untrusted Data	from n/a through <= 2.2.0	https://patchstack.com/database/Wordpress/Plugin/ulisting/vulnerability/wordpress-ulisting-plugin-2-2-0-php-object-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-27692	7,1	iccDEV	Out-of-bounds Write	up to and including 2.3.1.4	https://github.com/InternationalColorConsortium/iccDEV/commit/29d088840b962a7cdd35993dfabc2cb35a049847 GitHub, Inc. Patch https://github.com/InternationalColorConsortium/iccDEV/issues/609 GitHub, Inc. Exploit Issue Tracking https://github.com/InternationalColorConsortium/iccDEV/pull/610 GitHub, Inc. Issue Tracking Patch https://github.com/InternationalColorConsortium/iccDEV/security/advisories/GHSA-3869-prw8

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 and Partners Release Guidance for Ongoing Global Exploitation of Cisco SD-WAN Systems	***CVE-2026-20127* and *CVE-2022-20775***	**https://www.cisa.gov/news-events/alerts/2026/02/25/cisa-and-partners-release-guidance-ongoing-global-exploitation-cisco-sd-wan-systems**
CISA Adds Two Known Exploited Vulnerabilities to Catalog	▪ **CVE-2022-20775 Cisco Catalyst SD-WAN Path Traversal Vulnerability** ▪ **CVE-2026-20127 Cisco Catalyst SD-WAN Controller and Manager Authentication Bypass Vulnerability**	**https://www.cisa.gov/news-events/alerts/2026/02/25/cisa-adds-two-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
44% Surge in App Exploits as AI Speeds Up Cyber-Attacks, IBM Finds	https://www.infosecurity-magazine.com/news/app-exploits-surge-ai-speeds/
Google Disrupts 'Prolific' and 'Elusive' China-Linked Global Hacking Campaign	https://www.infosecurity-magazine.com/news/google-prolific-china-hacking/
Exploitable Vulnerabilities Present in 87% of Organizations	https://www.infosecurity-magazine.com/news/exploitable-vulnerabilities-in-87/
Darktrace Flags 32 Million Phishing Emails in 2025 as Identity Attacks Intensify	https://www.infosecurity-magazine.com/news/32m-phishing-emails-detected-2025/
Aeternum Botnet Shifts Command Control to Polygon Blockchain	https://www.infosecurity-magazine.com/news/aeternum-botnet-c2-polygon/
Cisco SD-WAN Zero-Day Under Exploitation for 3 Years	https://www.darkreading.com/vulnerabilities-threats/cisco-sd-wan-zero-day-exploitation-3-years
OpenAI Confirms that Chinese Hackers Used ChatGPT to Launch Cyberattacks	https://cybersecuritynews.com/openai-confirms-that-chinese-hackers-used-chatgpt/
Kali Linux Integrates Claude AI for Penetration Testing via Model Context Protocol	https://cybersecuritynews.com/kali-linux-integrates-claude-ai/
Microsoft to Stop Support for Windows Server 2016 and Windows 10 2016	https://cybersecuritynews.com/microsoft-stop-support-windows-server-2016-and-windows-10-2016/

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
Claude Code Hacked to Achieve Full RCE and Hijacked Organization API keys	https://cybersecuritynews.com/claude-code-hacked/
1 Million Records from Dutch Telco Odido Published Online After Extortion Attempt	https://cybersecuritynews.com/odido-data-breach/
Google API Keys Expose Private Data Silently Through Gemini	https://cybersecuritynews.com/google-api-keys-gemini/
Zoom Update Scam Infected 1,437 Users to Deploy Surveillance Tools in 12 Days	https://cybersecuritynews.com/zoom-update-scam-infected-1437-users/
Google Disrupts Chinese Hackers Infrastructre which Breached 53 Telecom and Government Entities	https://cybersecuritynews.com/google-disrupts-chinese-hackers-infrastructre/
Hacker Jailbreaks Claude AI to Write Exploit Code and Steal Government Data	https://cybersecuritynews.com/claude-ai-exploited-2/
CISA Confirms Active Exploitation of FileZen Vulnerability	https://cybersecuritynews.com/cisa-confirms-active-exploitation-of-filezen-vulnerability/

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
Critical Juniper Networks PTX flaw allows full router takeover	https://www.bleepingcomputer.com/news/security/critical-juniper-networks-ptx-flaw-allows-full-router-takeover/
Zyxel warns of critical RCE flaw affecting over a dozen routers	https://www.bleepingcomputer.com/news/security/zyxel-warns-of-critical-rce-flaw-affecting-over-a-dozen-routers/
Cisco SD-WAN Zero-Day CVE-2026-20127 Exploited Since 2023 for Admin Access	https://thehackernews.com/2026/02/cisco-sd-wan-zero-day-cve-2026-20127.html
Claude Code Flaws Allow Remote Code Execution and API Key Exfiltration	https://thehackernews.com/2026/02/claude-code-flaws-allow-remote-code.html
CISA Confirms Active Exploitation of FileZen CVE-2026-25108 Vulnerability	https://thehackernews.com/2026/02/cisa-confirms-active-exploitation-of.html
Critical ServiceNow AI Platform Vulnerability Enables Remote Code Execution	https://cybersecuritynews.com/servicenow-ai-platform-vulnerability/
27 Years old Telnet Vulnerability Enables Attackers to Gain Root Access	https://cybersecuritynews.com/27-years-old-telnet-vulnerability/
PoC Released for Windows Vulnerability That Allows Attackers to Cause Unrecoverable BSOD Crashes	https://cybersecuritynews.com/windows-vulnerability-bsod-crashes/
Hackers Can Abuse Cortex XDR Live Terminal Feature for C2 Communications	https://cybersecuritynews.com/hackers-can-abuse-cortex-xdr-live-terminal/
GitHub Copilot Exploited to Perform Full Repository Takeover via Passive Prompt Injection	https://cybersecuritynews.com/github-copilot-exploited/
Threat Actors Exploit Apache ActiveMQ Server Vulnerability to Gain RDP Access and Deploy LockBit Ransomware	https://cybersecuritynews.com/threat-actors-exploit-apache-activemq-server-vulnerability/
Multiple Vulnerabilities in CPSD CryptoPro Secure Disk for BitLocker Allow Root Access and Credential Theft	https://cybersecuritynews.com/vulnerabilities-in-cpsd-cryptopro-secure-disk-for-bitlocker/
SolarWinds Critical Serv-U Vulnerabilities Enables Root Access	https://cybersecuritynews.com/solarwinds-serv-u-vulnerabilities-2/

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
Trend Micro warns of critical Apex One code execution flaws	https://www.bleepingcomputer.com/news/security/trend-micro-warns-of-critical-apex-one-rce-vulnerabilities/
SolarWinds Patches 4 Critical Serv-U 15.5 Flaws Allowing Root Code Execution	https://thehackernews.com/2026/02/solarwinds-patches-4-critical-serv-u.html
Cisco Patches Catalyst SD-WAN Zero-Day Exploited by Highly Sophisticated Hackers	https://www.securityweek.com/cisco-patches-catalyst-sd-wan-zero-day-exploited-by-highly-sophisticated-hackers/
SolarWinds Patches Four Critical Serv-U Vulnerabilities	https://www.securityweek.com/solarwinds-patches-four-critical-serv-u-vulnerabilities/
Wireshark 4.6.4 Released With Fix for Multiple Security Vulnerabilities	https://cybersecuritynews.com/wireshark-4-6-4-released/

Firefox 148 Released With Sanitizer API to Disable XSS Attack	https://cybersecuritynews.com/firefox-148-released-with-sanitizer/
Microsoft Released Updates for Windows 11, Version 25H2 and 24H2 Systems	https://cybersecuritynews.com/microsoft-released-updates-for-windows-11-25h2-and-24h2/

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
Malicious NuGet Package Targets Stripe Developers	https://www.infosecurity-magazine.com/news/malicious-nuget-package-stripe-devs/
North Korean APT37 Hackers Leverages Novel Malware to Infect Air-Gapped Sys-tems	**https://cybersecuritynews.com/north-korean-apt37-hackers-leverages-novel-malware/**
Phishing-Led Agent Tesla Campaign Uses Process Hollowing and Anti-Analysis to Evade Detection	https://cybersecuritynews.com/phishing-led-agent-tesla-campaign/
ResidentBat Android Malware Provides Belarusian KGB with Persistent Access to Mobile Devices	https://cybersecuritynews.com/residentbat-android-malware/
New $300 Android RAT With Automated Permission Bypass and Hidden Remote Control	https://cybersecuritynews.com/new-300-android-rat/
DarkCloud Infostealer Emerges as Major Threat With Scalable Credential Theft Targeting Enterprises	https://cybersecuritynews.com/darkcloud-infostealer-emerges-as-major-threat/
Sophisticated SeaFlower Backdoor Campaign Targets Web3 Wallets to Steal Seed Phrases	https://cybersecuritynews.com/sophisticated-seaflower-backdoor-campaign-targets-web3-wallets/
Steaelite RAT Fuels New Wave of Double Extortion Threats Targeting Enterprises	https://cybersecuritynews.com/steaelite-rat-fuels-new-wave/
Microsoft Warns of Hackers Attacking Developers with Malicious Next.js Reposito-ries	https://cybersecuritynews.com/malicious-next-js-repositories/
OAuth Attacks in Entra ID Can Leverage ChatGPT to Compromise User Email Ac-counts	https://cybersecuritynews.com/oauth-attacks-in-entra-id-can-leverage-chatgpt/
Threat Actors Using Fake Avast Website to Harvest Users Credit Card Details	https://cybersecuritynews.com/threat-actors-using-fake-avast-website/

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/

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/