NATIONAL CYBERSECURITY AUTHORITY GR

CVEs Alerts

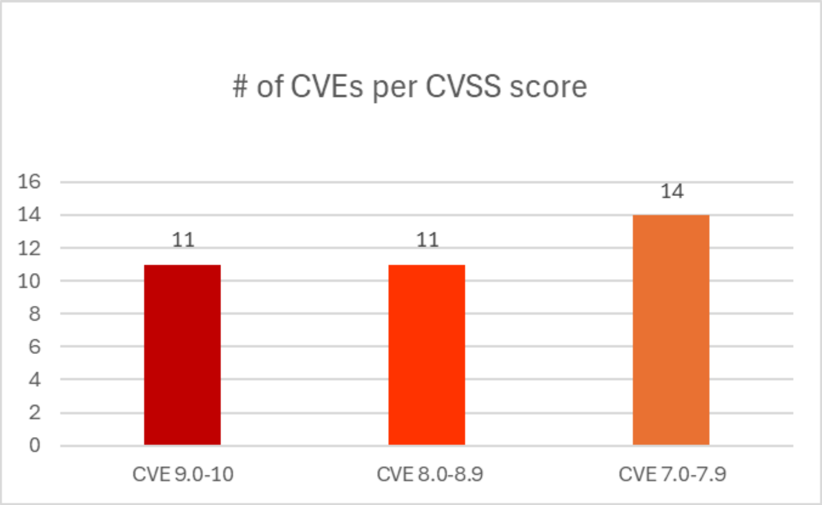
CVEs, CISA/CERT-EU Alerts Advisories & News

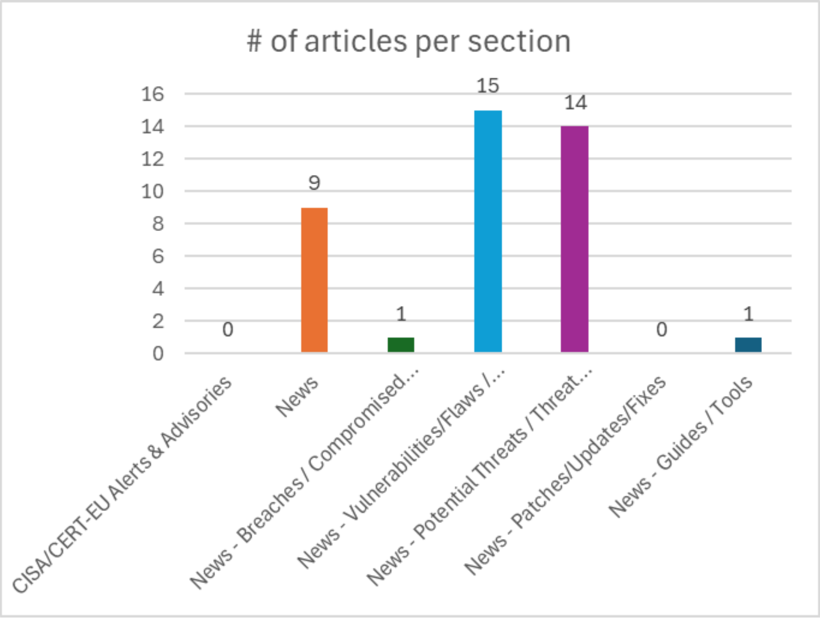
Newsletter on system vulnerabilities and cybersecurity news

Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 16/01/2026 - 20/01/2026





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-2026-23800	10,0	Modular DS	Incorrect Privilege Assignment	from 2.5.2 before 2.6.0	https://patchstack.com/database/wordpress/plugin/modular-connector/vulnerability/wordpress-modular-ds-plugin-2-5-2-privilege-escalation-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-22797	9,9	OpenStack	Authentication Bypass by Spoofing	10.5 through 10.7 before 10.7.2, 10.8 and 10.9 before 10.9.1, and 10.10 through 10.12 before 10.12.1	http://www.openwall.com/lists/oss-security/2026/01/15/1 http://www.openwall.com/lists/oss-security/2026/01/16/2 http://www.openwall.com/lists/oss-security/2026/01/16/3 http://www.openwall.com/lists/oss-security/2026/01/16/9 https://launchpad.net/bugs/2129018 https://www.openwall.com/lists/oss-security/2026/01/16/9
https://nvd.nist.gov/vuln/detail/CVE-2026-23836	9,9	HotCRP	Improper Input Validation	version 3.1	https://github.com/kohler/hotcrp/commit/4674fcfbb76511072a1145dad620756fc1d4b4e9 https://github.com/kohler/hotcrp/commit/bfc7e0db15df6ed6d544a639020d2ce05a5f0834 https://github.com/kohler/hotcrp/security/advisories/GHSA-hpqh-j6qx-x57h
https://nvd.nist.gov/vuln/detail/CVE-2025-60021	9,8	Apache bRPC	Improper Neutralization of Special Elements used in a Command ('Command Injection')	all versions < 1.15.0	http://www.openwall.com/lists/oss-security/2026/01/16/4 https://lists.apache.org/thread/xy51d2fx6drzhfp92xptsx5845q7b37m
https://nvd.nist.gov/vuln/detail/CVE-2026-1162	9,8	UTT HiPER 810	Improper Restriction of Operations within the Bounds of	1.7.4-141218	https://github.com/cha0yang1/UTT810/blob/main/1.md https://github.com/cha0yang1/UTT810/blob/main/1.md#poc https://vuldb.com/?ctiid.341756 https://vuldb.com/?id.341756 https://vuldb.com/?submit.736511

			a Memory Buffer		
https://nvd.nist.gov/vuln/detail/CVE-2026-23744	9,8	MCPJam	Missing Authentication for Critical Function	Versions 1.4.2	https://github.com/MCPJam/inspector/commit/e6b9cf9d9e6c9cbec31493b1bdca3a1255fe3e7a https://github.com/MCPJam/inspector/security/advisories/GHSA-232v-j27c-5pp6
https://nvd.nist.gov/vuln/detail/CVE-2026-23837	9,8	MyTube	Incorrect Authorization	version 1.7.65	https://github.com/franklioxygen/MyTube/commit/f85ae9b0d6e4a6480c6af5b675a99069d08d496e https://github.com/franklioxygen/MyTube/security/advisories/GHSA-cmvj-g69f-8664
https://nvd.nist.gov/vuln/detail/CVE-2026-23523	9,6	Dive	Improper Control of Generation of Code ('Code Injection')	Prior to 0.13.0	https://github.com/OpenAgentPlatform/Dive/commit/a5162ac9eff366d8ea1215b8a47139a81a55a779 https://github.com/OpenAgentPlatform/Dive/security/advisories/GHSA-pjj5-f3wm-f9m8
https://nvd.nist.gov/vuln/detail/CVE-2026-1221	9,3	PrismX MX100 AP	Use of Hard-coded Credentials		https://www.twcert.org.tw/en/cp-139-10643-2f8d7-2.html https://www.twcert.org.tw/tw/cp-132-10642-3b808-1.html
https://nvd.nist.gov/vuln/detail/CVE-2026-23841	9,3	Movary	Improper Input Validation	versions prior to 0.70.0	https://github.com/leepeuker/movary/releases/tag/0.70.0 https://github.com/leepeuker/movary/security/advisories/GHSA-v877-x568-4v5v
https://nvd.nist.gov/vuln/detail/CVE-2025-14510	9,2	ABB Ability OPTIMAX	Incorrect Implementation of Authentication Algorithm	6.1, 6.2, from 6.3.0 before 6.3.1-251120, from 6.4.0 before 6.4.1-251120	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108472A1331&LanguageCode=en&DocumentPartId=&Action=Launch

https://nvd.nist.gov/vuln/detail/CVE-2021-47816	8,8	Thecus N4800Eco NAS Server	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')		http://www.thecus.com/ http://www.thecus.com/product.php?PROD_ID=83 https://docs.unsafe-inline.com/0day/thecus-n4800eco-nas-server-control-panel-comand-injection https://www.exploit-db.com/exploits/49926 https://www.vulncheck.com/advisories/thecus-neco-nas-server-control-panel-command-injection
https://nvd.nist.gov/vuln/detail/CVE-2026-1140	8,8	UTT 进取 520W	Improper Restriction of Operations within the Bounds of a Memory Buffer	1.7.7-180627	https://github.com/cymiao1978/cve/blob/main/new/35.md https://vuldb.com/?ctiid.341731 https://vuldb.com/?id.341731 https://vuldb.com/?submit.735300
https://nvd.nist.gov/vuln/detail/CVE-2026-1158	8,8	Totolink LR350	Improper Restriction of Operations within the Bounds of a Memory Buffer		https://lavender-bicycle-a5a.notion.site/TOTOLINK-LR350-setWizardCfg-2e453a41781f80ce89cfc1d25049e279?source=copy_link https://vuldb.com/?ctiid.341752 https://vuldb.com/?id.341752 https://vuldb.com/?submit.735728 https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-20759	8,8	TRIFORA	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')		https://jvn.jp/en/jp/JVN08087148/ https://www.toa-products.com/securityinfo/pdf/tv2025-001jp.pdf

https://nvd.nist.gov/vuln/detail/CVE-2026-23742	8,8	Skipper	Improper Control of Generation of Code ('Code Injection')	before 0.23.0	https://github.com/zalando/skipper/commit/0b52894570773b29e2f3c571b94b4211ef8fa714 https://github.com/zalando/skipper/releases/tag/v0.23.0 https://github.com/zalando/skipper/security/advisories/GHSA-cc8m-98fm-rc9g
https://nvd.nist.gov/vuln/detail/CVE-2026-0695	8,7	ConnectWise PSA	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	versions older than 2026.1	https://www.connectwise.com/company/trust/security-bulletins/2026-01-15-psa-security-fix
https://nvd.nist.gov/vuln/detail/CVE-2026-23625	8,7	OpenProject	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Versions 16.3.0 through 16.6.4	https://github.com/opf/openproject/releases/tag/v16.6.5 https://github.com/opf/openproject/releases/tag/v17.0.0 https://github.com/opf/openproject/security/advisories/GHSA-cvpq-cc56-gwxx
https://nvd.nist.gov/vuln/detail/CVE-2026-23735	8,7	GraphQL	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	From 2.2.1 to before 2.4.1 and 3.1.1	https://github.com/graphql-hive/graphql-modules/issues/2613 https://github.com/graphql-hive/graphql-modules/pull/2521 https://github.com/graphql-hive/graphql-modules/releases/tag/release-1768575025568 https://github.com/graphql-hive/graphql-modules/security/advisories/GHSA-53wg-r69p-v3r7
https://nvd.nist.gov/vuln/detail/CVE-2026-22865	8,6	Gradle	Download of Code	versions before 9.3.0	https://github.com/gradle/gradle/security/advisories/GHSA-mqwm-5m85-gmcv

			Without Integrity Check		
https://nvd.nist.gov/vuln/detail/CVE-2026-23876	8,1	ImageMagick	Heap-based Buffer Overflow	versions 7.1.2-13 and 6.9.13-38	https://github.com/ImageMagick/ImageMagick/commit/2fae24192b78fdfdd27d766fd21d90aeac6ea8b8 https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-r49w-jqq3-3gx8
https://nvd.nist.gov/vuln/detail/CVE-2026-20960	8,0	Microsoft Power Apps	Improper Authorization		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-20960
https://nvd.nist.gov/vuln/detail/CVE-2021-47826	7,8	Acer Backup Manager	Unquoted Search Path or Element	3.0.0.99	https://www.acer.com/ac/en/US/content/home https://www.exploit-db.com/exploits/49889 https://www.vulncheck.com/advisories/acer-backup-manager-module-ischedulesvcexe-unquoted-service-path
https://nvd.nist.gov/vuln/detail/CVE-2021-47828	7,8	BOOTP Turbo	Unquoted Search Path or Element	2.0.0.1253	https://www.exploit-db.com/exploits/49851 https://www.vulncheck.com/advisories/bootp-turbo-bootptexe-unquoted-service-path https://www.weird-solutions.com
https://nvd.nist.gov/vuln/detail/CVE-2021-47829	7,8	DHCP Broadband	Unquoted Search Path or Element	4.1.0.1503	https://www.exploit-db.com/exploits/49850 https://www.vulncheck.com/advisories/dhcp-broadband-dhcptexe-unquoted-service-path https://www.weird-solutions.com
https://nvd.nist.gov/vuln/detail/CVE-2021-47833	7,8	WifiHotSpot	Unquoted Search Path or Element	1.0.0.0	https://wifi-hotspot.gearboxcomputers.com/ https://www.exploit-db.com/exploits/49845 https://www.vulncheck.com/advisories/wifihotspot-wifihotspotserviceexe-unquoted-service-path
https://nvd.nist.gov/vuln/detail/CVE-2021-47845	7,8	Spy Emergency	Unquoted Search Path or Element	25.0.650	https://www.exploit-db.com/exploits/49997 https://www.spy-emergency.com/ https://www.vulncheck.com/advisories/spy-emergency-unquoted-service-path
https://nvd.nist.gov/vuln/detail/CVE-2021-47847	7,8	Disk Sorter Server	Unquoted Search Path or Element	13.6.12	https://www.disksorter.com https://www.exploit-db.com/exploits/50013 https://www.vulncheck.com/advisories/disk-sorter-server-disk-sorter-server-unquoted-service-path

https://nvd.nist.gov/vuln/detail/CVE-2026-23529	7,7	Kafka	External Control of File Name or Path	Prior to 2.11.0	https://docs.cloud.google.com/support/bulletins#gcp-2025-005 https://github.com/Aiven-Open/bigquery-connector-for-apache-kafka/commit/20ea3921c6fe72d605a033c1943b20f49eaba981 https://github.com/Aiven-Open/bigquery-connector-for-apache-kafka/releases/tag/v2.11.0 https://github.com/Aiven-Open/bigquery-connector-for-apache-kafka/security/advisories/GHSA-3mg8-2g53-5gj4
https://nvd.nist.gov/vuln/detail/CVE-2021-47827	7,5	WebSSH	mproper Validation of Specified Quantity in Input	iOS 14.16.10	https://apps.apple.com/mx/app/webssh-ssh-client/id497714887 https://www.exploit-db.com/exploits/49883 https://www.vulncheck.com/advisories/webssh-for-ios-mashrepl-denial-of-service
https://nvd.nist.gov/vuln/detail/CVE-2025-14894	7,5	Livewire Filemanager			https://github.com/livewire-filemanager/filemanager https://hackingbydoing.wixsite.com/hackingbydoing/post/unauthenticated-rce-in-livewire-filemanager https://www.kb.cert.org/vuls/id/650657
https://nvd.nist.gov/vuln/detail/CVE-2025-68675	7,5	Apache Airflow	Insertion of Sensitive Information into Log File	versions before 3.1.6	http://www.openwall.com/lists/oss-security/2026/01/15/6 https://lists.apache.org/thread/x6kply4nqd4vc4wgxtm6g9r2tt63s8c5
https://nvd.nist.gov/vuln/detail/CVE-2026-23842	7,5	ChatterBot	ncontrolled Resource Consumption	versions up to 1.2.10	https://github.com/gunthercox/ChatterBot/commit/de89fe648139f8eeacc998ad4524fab291a378cf https://github.com/gunthercox/ChatterBot/pull/2432 https://github.com/gunthercox/ChatterBot/releases/tag/1.2.11 https://github.com/gunthercox/ChatterBot/security/advisories/GHSA-v4w8-49pv-mf72 https://github.com/user-attachments/assets/4ee845c4-b847-4854-84ec-4b2fb2f7090f
https://nvd.nist.gov/vuln/detail/CVE-2026-1125	7,3	D-Link	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')		https://github.com/DavCloudz/cve/blob/main/D-link/DIR_823X/DIR-823X%20V250416%20Command%20Execution%20Vulnerability.md https://vuldb.com/?ctiid.341717 https://vuldb.com/?id.341717 https://vuldb.com/?submit.734966 https://www.dlink.com/

https://nvd.nist.gov/vuln/detail/CVE-2025-12007	7,2	Supermicro BMC	Improper Verification of Cryptographic Signature		https://www.supermicro.com/en/support/security_BMC_IPMI_Jan_2026
https://nvd.nist.gov/vuln/detail/CVE-2025-24528	7,1	MIT Kerberos 5 (aka krb5)	Integer Overflow or Wraparound	before 1.22	https://github.com/krb5/krb5/commit/78ceba024b64d49612375be4a12d1c066b0bfbd0 https://github.com/krb5/krb5/compare/krb5-1.21.3-final...krb5-1.22-final https://lists.debian.org/debian-lts-announce/2025/02/msg00029.html

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

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
ChatGPT Go Launched for $8 USD/month With Support for Ads and Privacy Risks	https://cybersecuritynews.com/chatgpt-go-with-support-for-ads/
Free Converter Apps that Convert your Clean System to Infected in Seconds	https://cybersecuritynews.com/free-converter-apps-infect-systems/
Microsoft January 2026 Security Update Causes Credential Prompt Failures in Remote Desktop Connections	https://cybersecuritynews.com/remote-desktop-connections-prompt-failures/
Mandiant Releases Rainbow Tables Enabling NTLMv1 Admin Password Hacking	https://cybersecuritynews.com/rainbow-tables-enabling-ntlmv1-hack/
Let’s Encrypt has made 6-day IP-based TLS certificates Generally Available	https://cybersecuritynews.com/lets-encrypt-6-day-tls-certificates/
Argus – Python-powered Toolkit for Information Gathering and Reconnaissance	https://cybersecuritynews.com/argus-python-toolkit/
Researchers Gain Access to StealC Malware Command-and-Control Systems	https://cybersecuritynews.com/researchers-gain-access-to-stealc-malware-command-and-control-systems/
Windows 11 PCs Fail to Shut Down After January Security Update	https://cybersecuritynews.com/windows-11-pcs-fail-to-shut-down/
Cloudflare Acquired Open-source Web Framework Astro to Supercharge Development	https://cybersecuritynews.com/cloudflare-acquired-astro/

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
CIRO Confirms Data Breach – 750,000 Canadian Investors Have been Impacted	https://cybersecuritynews.com/ciro-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
Critical AVEVA Software Vulnerabilities Enables Remote Code Execution Under System Privileges	https://cybersecuritynews.com/aveva-software-vulnerabilities/
WhisperPair Attack Allows Hijacking of Laptops, Earbuds Without User Consent – Millions Affected	https://cybersecuritynews.com/whisperpair-attack/
Pulsar RAT Using Memory-Only Execution & HVNC to Gain Invisible Remote Access	https://cybersecuritynews.com/pulsar-rat-gain-remote-access/
Apache bRPC Vulnerability Enables Remote Command Injection	https://cybersecuritynews.com/apache-brpc-vulnerability-2/
Google Gemini Privacy Controls Bypassed to Access Private Meeting Data Using Calendar Invite	https://cybersecuritynews.com/gemini-privacy-controls-bypassed/
Cloudflare Zero-Day Vulnerability Enables Any Host Access Bypassing Protections	https://cybersecuritynews.com/cloudflare-zero-day-vulnerability/
Livewire Filemanager Vulnerability Exposes Web Applications to RCE Attacks	https://cybersecuritynews.com/livewire-filemanager-vulnerability/
Windows SMB Client Vulnerability Enables Attacker to Own Active Directory	https://cybersecuritynews.com/windows-smb-client-vulnerability/
Redmi Buds Vulnerability Allow Attackers Access Call Data and Trigger Firmware Crashes	https://cybersecuritynews.com/redmi-buds-vulnerability/
New Kerberos Relay Attack Uses DNS CNAME to Bypass Mitigations – PoC Released	https://cybersecuritynews.com/kerberos-relay-attack-uses-dns-cname/
BodySnatcher – New Vulnerability Allows Attacker to Impersonate Any ServiceNow User	https://cybersecuritynews.com/bodysnatcher-vulnerability-impersonate-servicenow-user/
Google's Vertex AI Vulnerability Enables Low-Privileged Users to Gain Service Agent Roles	https://cybersecuritynews.com/google-vertex-ai-vulnerability/
Cisco 0-Day RCE Secure Email Gateway Vulnerability Exploited in the Wild	https://cybersecuritynews.com/cisco-0-day-rce-secure-email-gateway-vulnerability/
Go 1.25.6 and 1.24.12 Patch Critical Vulnerabilities Lead to DoS and Memory Exhaustion Risks	https://cybersecuritynews.com/go-1-25-6-and-1-24-12-vulnerabilities/
New AWS Console Supply Chain Attack Allows Hijack of AWS GitHub Repositories	https://cybersecuritynews.com/aws-console-supply-chain-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

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
Attackers Abuse Discord to Deliver Clipboard Hijacker That Steals Wallet Addresses on Paste	https://cybersecuritynews.com/attackers-abuse-discord-to-deliver-clipboard-hijacker/
Python-based Malware SolyxImmortal Leverages Discord to Silently Harvest Sensitive Data	https://cybersecuritynews.com/python-based-malware-solyximmortal-leverages-discord/
Threat Actors Leverage Google Ads to Weaponize PDF Editor with TamperedChef	https://cybersecuritynews.com/threat-actors-leverage-google-ads/
Remcos RAT Masquerade as VeraCrypt Installers Steals Users Login Credentials	https://cybersecuritynews.com/remcos-rat-masquerade-as-veracrypt-installers/
Threat Actors Weaponizing Visual Studio Code to Deploy a Multistage Malware	https://cybersecuritynews.com/threat-actors-weaponizing-visual-studio-code/
Inside the Leaks that Exposed the Hidden Infrastructure Behind a Ransomware Operation	https://cybersecuritynews.com/inside-the-leaks-that-exposed-the-hidden-infrastructure/
Threat Actors Impersonate as MalwareBytes to Attack Users and Steal Logins	https://cybersecuritynews.com/threat-actors-impersonate-as-malwarebytes/
Attackers are Using WSL2 as a Stealthy Hideout Inside Windows Systems	https://cybersecuritynews.com/attackers-are-using-wsl2-as-a-stealthy-hideout/
New Spear-Phishing Attack Abusing Google Ads to Deliver EndRAT Malware	https://cybersecuritynews.com/new-spear-phishing-attack-abusing-google-ads/
5 Malicious Chrome Extensions Attacking Enterprise HR and ERP Platforms for Complete Takeover	https://cybersecuritynews.com/5-malicious-chrome-extensions-attacking-enterprise-hr/
PDFSIDER Malware Actively Used by Threat Actors to Bypass Antivirus and EDR Systems	https://cybersecuritynews.com/pdfsider-malware-actively-used-by-threat-actors/
Researchers Gained Access to Hacker Domain Server Using Name Server Delegation	https://cybersecuritynews.com/researchers-gained-access-to-hacker-domain-server/
CrashFix – Hackers Using Malicious Extensions to Display Fake Browser Warnings	https://cybersecuritynews.com/crashfix-hackers-using-malicious-extensions/
17 New Malicious Chrome GhostPoster Extensions with 840,000+ Installs Steals User Data	https://cybersecuritynews.com/17-new-malicious-chrome-ghostposter-extensions/

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 15 Best Ethical Hacking Tools – 2026	https://cybersecuritynews.com/ethical-hacking-tools/

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/