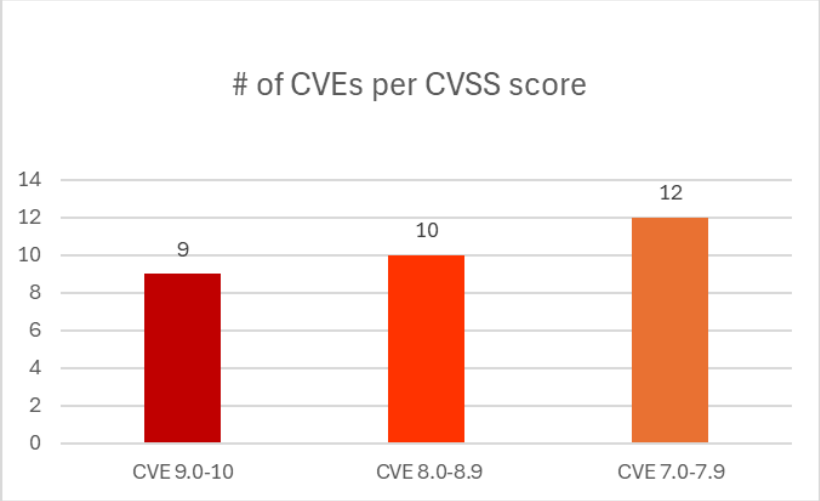
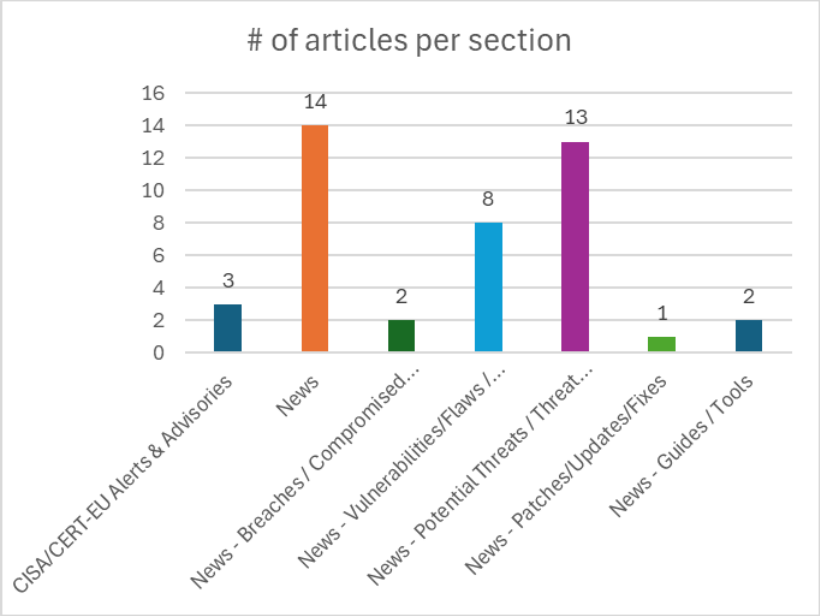
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 14/03/2026 - 17/03/2026





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-2016-20024	**9,8**	ZKTeco	Insertion of Sensitive Information into Externally-Accessible File or Directory	ZKTeco ZKTime.Net 3.0.1.6	https://cxsecurity.com/issue/WLB-2016080264 https://exchange.xforce.ibmcloud.com/vulnerabilities/116487 https://packetstormsecurity.com/files/138565 https://www.exploit-db.com/exploits/40322/ https://www.vulncheck.com/advisories/zkteco-zktime-net-insecure-file-permissions-privilege-escalation https://www.zeroscience.mk/en/vulnerabilities/ZSL-2016-5360.php
https://nvd.nist.gov/vuln/detail/CVE-2016-20030	**9,8**	ZKTeco	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	ZKTeco ZKBioSecurity 3.0	https://exchange.xforce.ibmcloud.com/vulnerabilities/116485 https://packetstormsecurity.com/files/138573 https://www.vulncheck.com/advisories/zkteco-zkbiosecurity-user-enumeration-via-authloginaction https://www.zeroscience.mk/en/vulnerabilities/ZSL-2016-5366.php
https://nvd.nist.gov/vuln/detail/CVE-2017-20223	**9,8**	Telesquare	Authorization Bypass Through User-Controlled Key	Telesquare SKT LTE Router SDT-CS3B1 firmware version 1.2.0	https://cxsecurity.com/issue/WLB-2017120297 https://exchange.xforce.ibmcloud.com/vulnerabilities/136993 https://packetstormsecurity.com/files/145551 https://www.exploit-db.com/exploits/43402/ https://www.vulncheck.com/advisories/telesquare-skt-lte-router-sdt-cs3b1-insecure-direct-object-reference

					https://www.zeroscience.mk/en/vulnerabilities/ZSL-2017-5445.php
https://nvd.nist.gov/vuln/detail/CVE-2017-20224	9,8	Telesquare	Unrestricted Upload of File with Dangerous Type	Telesquare SKT LTE Router SDT-CS3B1 version 1.2.0	https://cxsecurity.com/issue/WLB-2017120301 https://www.vulncheck.com/advisories/telesquare-skt-lte-router-sdt-cs3b1-webdav-arbitrary-file-upload https://www.zeroscience.mk/en/vulnerabilities/ZSL-2017-5446.php
https://nvd.nist.gov/vuln/detail/CVE-2026-4164	9,8	Wavlink	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	Wavlink WL-WN578W2 221110	https://dl.wavlink.com/firmware/RD/WINSTAR_WN578W2-A-2026-03-10-94f93d4-WO-mt7628-squashfs-sysupgrade.bin https://github.com/Litengzheng/vul_db/blob/main/WL-WN578W2/vul_1/README.md https://github.com/Litengzheng/vul_db/blob/main/WL-WN578W2/vul_2/README.md https://vuldb.com/?ctiid.351071 https://vuldb.com/?id.351071 https://vuldb.com/?submit.768292 https://vuldb.com/?submit.768293 https://vuldb.com/?submit.768294
https://nvd.nist.gov/vuln/detail/CVE-2026-4170	9,8	Topsec	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Topsec TopACM 3.0	https://my.feishu.cn/docx/EAFFdhzoeodDxfxeazNcxBzCnRf?from=from_copylink https://vuldb.com/?ctiid.351077 https://vuldb.com/?id.351077 https://vuldb.com/?submit.769768
https://nvd.nist.gov/vuln/detail/CVE-2026-4184	9,8	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	D-Link DIR-816 1.10CNB05	https://github.com/wudipjq/my_vuln/blob/main/D-Link7/vuln_88/88.md https://vuldb.com/?ctiid.351088 https://vuldb.com/?id.351088 https://vuldb.com/?submit.769832 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-4254	9,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda AC8 up to 16.03.50.11	https://github.com/digitalandrew/tenda_ac8_v5/blob/main/CVE_Report_Tenda_AC8_SysToolChangePwd_BOF.md https://vuldb.com/?ctiid.351212 https://vuldb.com/?id.351212 https://vuldb.com/?submit.771773 https://www.tenda.com.cn/

https://nvd.nist.gov/vuln/detail/CVE-2026-27962	9,1	Authlib is a Python library	Improper Verification of Cryptographic Signature	Prior to version 1.6.9	https://github.com/authlib/authlib/commit/a5d4b2d4c9e46bfa11c82f85fdc2bcc0b50ae681 https://github.com/authlib/authlib/releases/tag/v1.6.9 GitHub https://github.com/authlib/authlib/security/advisories/GHSA-wvwj-cvrp-7pv5
https://nvd.nist.gov/vuln/detail/CVE-2016-20025	8,8	ZKTeco	Files or Directories Accessible to External Parties	ZKTeco ZKAccess Professional 3.5.3	https://cxsecurity.com/issue/WLB-2016080265 https://exchange.xforce.ibmcloud.com/vulnerabilities/11648 https://packetstormsecurity.com/files/138566 https://www.exploit-db.com/exploits/40323/ https://www.vulncheck.com/advisories/zkteco-zkaccess-professional-privilege-escalation-via-insecure-permissions https://www.zeroscience.mk/en/vulnerabilities/ZSL-2016-5361.php
https://nvd.nist.gov/vuln/detail/CVE-2026-4167	8,8	Belkin	Improper Restriction of Operations within the Bounds of a Memory Buffer	Belkin F9K1122 1.00.33	https://github.com/Litengzheng/vul_db/blob/main/Belkin/vul_152/README.md https://github.com/Litengzheng/vul_db/blob/main/Belkin/vul_152/README.md#proof-of-concept-poc https://vuldb.com/?ctiid.351074 https://vuldb.com/?id.351074 https://vuldb.com/?submit.769727
https://nvd.nist.gov/vuln/detail/CVE-2026-4188	8,8	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	A security flaw has been discovered in D-Link DIR-619L 2.06B01	https://github.com/wudipjq/my_vuln/blob/main/D-Link7/vuln_89/89.md https://vuldb.com/?ctiid.351094 https://vuldb.com/?id.351094 https://vuldb.com/?submit.769833 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-4211	8,8	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	A weakness has been identified in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20260205	https://github.com/wudipjq/my_vuln/blob/main/D-Link8/vuln_160/160.md https://vuldb.com/?ctiid.351122 https://vuldb.com/?id.351122 https://vuldb.com/?submit.770441 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-4212	8,8	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	A security vulnerability has been detected in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20260205	https://github.com/wudipjq/my_vuln/blob/main/D-Link8/vuln_161/161.md https://vuldb.com/?ctiid.351123 https://vuldb.com/?id.351123

					https://vuldb.com/?submit.770442 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-4213	**8,8**	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	A vulnerability was detected in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20260205	https://github.com/wudipjq/my_vuln/blob/main/D-Link8/vuln_162/162.md https://github.com/wudipjq/my_vuln/blob/main/D-Link8/vuln_163/163.md https://vuldb.com/?ctiid.351124 https://vuldb.com/?id.351124 https://vuldb.com/?submit.770443 https://vuldb.com/?submit.770444 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-4214	**8,8**	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	A flaw has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20260205	https://github.com/wudipjq/my_vuln/blob/main/D-Link8/vuln_164/164.md https://vuldb.com/?ctiid.351125 https://vuldb.com/?id.351125 https://vuldb.com/?submit.770445 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-4227	**8,8**	LB-LINK	Improper Restriction of Operations within the Bounds of a Memory Buffer	LB-LINK BL-WR9000 2.4.9	https://github.com/glkfc/IoT-Vulnerability/blob/main/LB-LINK/LB-LINK_HideSSID%20stack%20overflow_EN.md https://vuldb.com/?ctiid.351150 https://vuldb.com/?id.351150 https://vuldb.com/?submit.771209
https://nvd.nist.gov/vuln/detail/CVE-2026-32600	**8,2**	xml-security	Improper Validation of Integrity Check Value	xml-security is a library that implements XML signatures and encryption. Prior to versions 2.3.1 and 1.13.9	https://github.com/simplesamlphp/xml-security/commit/cad6d57cf0a5a0b7e0cc4e4a5b18752e56eb1520 https://github.com/simplesamlphp/xml-security/commit/fdc12449e959c610943f9fd428e95e3832d74c25 https://github.com/simplesamlphp/xml-security/security/advisories/GHSA-r353-4845-pr5p
https://nvd.nist.gov/vuln/detail/CVE-2026-32616	**8,2**	Pigeon	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	Pigeon is a message board/notepad/social system/blog. Prior to 1.0.201	https://github.com/kasuganosoras/Pigeon/releases/tag/1.0.201 https://github.com/kasuganosoras/Pigeon/security/advisories/GHSA-rrj4-9wgq-prcr
https://nvd.nist.gov/vuln/detail/CVE-2026-23862	**7,8**	Dell	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Dell ThinOS 10 versions prior to ThinOS 2602_10.0573	https://www.dell.com/support/kbdoc/en-us/000435801/dsa-2026-122

https://nvd.nist.gov/vuln/detail/CVE-2026-3476	**7,8**	SOLIDWORKS	Improper Control of Generation of Code ('Code Injection')	SOLIDWORKS Desktop from Release 2025 through Release 2026	https://www.3ds.com/trust-center/security/security-advisories/cve-2026-3476
https://nvd.nist.gov/vuln/detail/CVE-2026-2476	**7,6**	Mattermost	Exposure of Sensitive Information to an Unauthorized Actor	Mattermost Plugins versions <=2.0.3.0	https://mattermost.com/security-updates
https://nvd.nist.gov/vuln/detail/CVE-2017-20222	**7,5**	Telesquare	Missing Authentication for Critical Function	Telesquare SKT LTE Router SDT-CS3B1 software version 1.2.0	https://cxsecurity.com/issue/WLB-2017120300 https://exchange.xforce.ibmcloud.com/vulnerabilities/136825 https://packetstormsecurity.com/files/145555 https://www.exploit-db.com/exploits/43401/ https://www.vulncheck.com/advisories/telesquare-skt-lte-router-sdt-cs3b1-unauthenticated-remote-reboot https://www.zeroscience.mk/en/vulnerabilities/ZSL-2017-5444.php
https://nvd.nist.gov/vuln/detail/CVE-2026-24458	**7,5**	Mattermost	Allocation of Resources Without Limits or Throttling	Mattermost versions 11.3.x <= 11.3.0, 11.2.x <= 11.2.2, 10.11.x <= 10.11.10	https://mattermost.com/security-updates
https://nvd.nist.gov/vuln/detail/CVE-2026-4180	**7,3**	D-Link	Incorrect Privilege Assignment	D-Link DIR-816 1.10CNB05	https://github.com/wudipjq/my_vuln/blob/main/D-Link7/vuln_84/84.md https://vuldb.com/?ctiid.351084 https://vuldb.com/?id.351084 https://vuldb.com/?submit.769828 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-4193	**7,3**	D-Link	Incorrect Privilege Assignment	A security vulnerability has been detected in D-Link DIR-823G 1.0.2B05	https://github.com/wudipjq/my_vuln/blob/main/D-Link7/vuln_91/91.md https://github.com/wudipjq/my_vuln/blob/main/D-Link7/vuln_92/92.md https://vuldb.com/?ctiid.351105 https://vuldb.com/?id.351105 https://vuldb.com/?submit.769835 https://vuldb.com/?submit.769836 https://vuldb.com/?submit.769837 https://vuldb.com/?submit.769838 https://vuldb.com/?submit.769839 https://vuldb.com/?submit.769841 https://www.dlink.com/

https://nvd.nist.gov/vuln/detail/CVE-2026-4194	**7,3**	D-Link	Incorrect Privilege Assignment	A vulnerability was detected in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20260205	https://github.com/wudipjq/my_vuln/blob/main/D-Link8/vuln_96/96.md https://vuldb.com/?ctiid.351106 https://vuldb.com/?id.351106 https://vuldb.com/?submit.769853 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-4232	**7,3**	Tiandy	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	Tiandy Integrated Management Platform 7.17.0	https://my.feishu.cn/docx/UxbzdoU7coxKGjxbJ7ycPor3n3Q?from=from_copylink https://vuldb.com/?ctiid.351155 https://vuldb.com/?id.351155 https://vuldb.com/?submit.771216
https://nvd.nist.gov/vuln/detail/CVE-2016-20032	**7,2**	ZKTeco	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	ZKTeco ZKAccess Security System 5.3.1	https://cxsecurity.com/issue/WLB-2016090004 https://exchange.xforce.ibmcloud.com/vulnerabilities/116479 https://packetstormsecurity.com/files/138572 https://www.exploit-db.com/exploits/40328/ https://www.vulncheck.com/advisories/zkteco-zkaccess-security-system-stored-xss https://www.zeroscience.mk/en/vulnerabilities/ZSL-2016-5368.php
https://nvd.nist.gov/vuln/detail/CVE-2026-4172	**7,2**	TRENDnet	Improper Restriction of Operations within the Bounds of a Memory Buffer	TRENDnet TEW-632BRP 1.010B32	https://github.com/i-Corner/cve/issues/40 https://vuldb.com/?ctiid.351079 https://vuldb.com/?id.351079 https://vuldb.com/?submit.769770
https://nvd.nist.gov/vuln/detail/CVE-2026-26133	**7,1**	M365 Copilot		AI command injection in M365 Copilot allows an unauthorized attacker to disclose information over a network.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26133

CISA/CERT-EU Alerts & Advisories

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

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds Two Known Exploited Vulnerabilities to Catalog	▪ CVE-2026-3909 Google Skia Out-of-Bounds Write Vulnerability ▪ CVE-2026-3910 Google Chromium V8 Unspecified Vulnerability	https://www.cisa.gov/news-events/alerts/2026/03/13/cisa-adds-two-known-exploited-vulnerabilities-catalog
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2025-47813 Wing FTP Server Information Disclosure Vulnerability	https://www.cisa.gov/news-events/alerts/2026/03/16/cisa-adds-one-known-exploited-vulnerability-catalog
V1: ED 26-03: Mitigate Vulnerabilities in Cisco SD-WAN Systems		https://www.cisa.gov/news-events/directives/v1-ed-26-03-mitigate-vulnerabilities-cisco-sd-wan-systems

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
Stryker Confirms Destructive Wiper Attack – Tens of Thousands of Devices Wiped	https://cybersecuritynews.com/stryker-wiper-attack/
Microsoft Exchange Online Mailbox Access Outage Affects Users Globally	https://cybersecuritynews.com/microsoft-exchange-online-mailbox-outage/
Android 17 Advanced Protection Mode to Block Malicious Service Usage	https://cybersecuritynews.com/android-17-advanced-protection-mode/
Google Looker Studio Vulnerabilities Allow Attackers to Exfiltrate Data from Google Services	https://cybersecuritynews.com/google-looker-studio-vulnerabilities/
Meta to Permanently Remove End-to-End Encryption Feature in Instagram DMs	https://cybersecuritynews.com/instagram-end-to-end-encryption/
FortiGate Firewalls Exploited in Wave of Attacks to Breach Networks and Steal Credentials	https://cybersecuritynews.com/fortigate-firewalls-exploited/
Malicious npm Packages Posing as Solara Executor Target Discord, Browsers, and Crypto Wallets	https://cybersecuritynews.com/malicious-npm-packages-target-discord-browsers-and-crypto-wallets/
Microsoft Confirms Windows 11 24H2/25H2 Bug Blocks Access to the System Drive C	https://cybersecuritynews.com/windows-11-bug-drive-c/
Metasploit Pro 5.0.0 Released With Powerful New Modules and Critical Enhancements	https://cybersecuritynews.com/metasploit-pro-5-0-0-released/
Chrome Zero-Day Vulnerabilities Actively Exploited in the Wild to Execute Malicious Code	https://cybersecuritynews.com/chrome-zero-day-vulnerabilities-actively-exploited/
Salesforce Warns of ShinyHunters Group Exploiting Experience Cloud Sites	https://cybersecuritynews.com/salesforce-warns-shinyhunters/

Qihoo 360 Leaked Its Own Wildcard SSL Private Key Inside Public AI Installer	https://cybersecuritynews.com/qihoo-360-leaked-ssl-private-key/
Authorities Crack Down on 45,000 Malicious IPs Powering Ransomware Attacks	https://cybersecuritynews.com/authorities-crack-down-on-45000-malicious-ips/
Authorities Dismantle Malicious Proxy Service Used to Deploy Malware Attacking Thousands of Users	https://cybersecuritynews.com/authorities-dismantle-malicious-proxy-service/

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
Loblaw Data Breach – Hackers Accessed IT Network and Customer Information	https://cybersecuritynews.com/loblaw-data-breach/
Starbucks Data Breach – Hundreds of Users' Personal Data Exposed	https://cybersecuritynews.com/starbucks-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
Researchers Decrypt and Exploit Encrypted Palo Alto Cortex XDR BIOC Rules	https://cybersecuritynews.com/decrypt-and-exploit-cortex-xdr/
OpenClaw AI Agents Leaking Sensitive Data in Indirect Prompt Injection Attacks	https://cybersecuritynews.com/openclaw-ai-agents-leak-sensitive-data/
Microsoft to Block Windows 11 and Server 2025 Automated Installation After Critical RCE Vulnerability	https://cybersecuritynews.com/windows-11-and-server-2025-automated-installation/
Microsoft Releases Out-of-Band Patch For Critical RRAS RCE Vulnerabilities in Windows 11	https://cybersecuritynews.com/windows-11-out-of-band-update/
Critical LangSmith Account Takeover Vulnerability Puts Users at Risk	https://cybersecuritynews.com/critical-langsmith-account-takeover-vulnerability/
Veeam Patches Multiple Critical RCE Vulnerabilities on Backup Server	https://cybersecuritynews.com/veeam-backup-server-vulnerabilities/
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/

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
Apple Released Emergency Updates for iOS 15.8.7 to Thwart 'Coruna' Exploit Kit	https://cybersecuritynews.com/apple-released-emergency-updates/

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
Malicious npm Packages Deliver PylangGhost RAT in New Software Supply Chain Campaign	https://cybersecuritynews.com/malicious-npm-packages-deliver-pylangghost-rat/
Phishers Abuse LiveChat Support Tools to Steal Sensitive Data in New SaaS-Based Attack Tactic	https://cybersecuritynews.com/phishers-abuse-livechat-support-tools/
New CondiBot Variant and 'Monaco' Cryptominer Expand Threats to Network Devices	https://cybersecuritynews.com/new-condibot-variant-and-monaco-cryptominer/
Handala Hack Uses RDP, NetBird, and Parallel Wipers in MOIS-Linked Destructive Intrusions	https://cybersecuritynews.com/handala-hack-uses-rdp/
CamelClone Spy Campaign Abuses Public File-Sharing Sites and Rclone in Government-Focused Attacks	https://cybersecuritynews.com/camelclone-spy-campaign/
RondoDox Botnet Expands to 174 Exploits, Leveraging Residential IP Infrastructure at Scale	https://cybersecuritynews.com/rondodox-botnet-expands/
Fake Shipment Tracking Scams Surge in MEA, Stealing Banking Data Through Real-Time Phishing	https://cybersecuritynews.com/fake-shipment-tracking-scams-surge-in-mea/
IBM Uncovers 'Slopoly,' Likely AI-Generated Malware Used in Hive0163 Ransomware Attack	https://cybersecuritynews.com/ibm-uncovers-slopoly-likely-ai-generated-malware/
Fake FileZilla Downloads Lead to RAT Infections Through Stealthy Multi-Stage Loader	https://cybersecuritynews.com/fake-filezilla-downloads-lead-to-rat-infections/
New ACRStealer Variant Uses Syscall Evasion, TLS C2 and Secondary Payload Delivery	https://cybersecuritynews.com/new-acrstealer-variant-uses-syscall-evasion/
Konni APT Hijacks KakaoTalk Accounts to Spread Malware in Multi-Stage Spear-Phishing Campaign	https://cybersecuritynews.com/konni-apt-hijacks-kakaotalk-accounts/
Attackers Abuse Microsoft Teams and Quick Assist to Drop Stealthy A0Backdoor	https://cybersecuritynews.com/attackers-abuse-microsoft-teams-to-drop-a0backdoor/
GlassWorm Campaign Uses 72 Malicious Open VSX Extensions to Broaden Reach	https://cybersecuritynews.com/glassworm-campaign-uses-72-malicious-open-vsx-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
Betterleaks – A New Open-Source Tool to Scan Directories, Files, and Git Repositories	https://cybersecuritynews.com/betterleaks-tool/
Meta Launches New Anti-Scam Tools on WhatsApp, Facebook and Messenger	https://cybersecuritynews.com/meta-new-anti-scam-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/