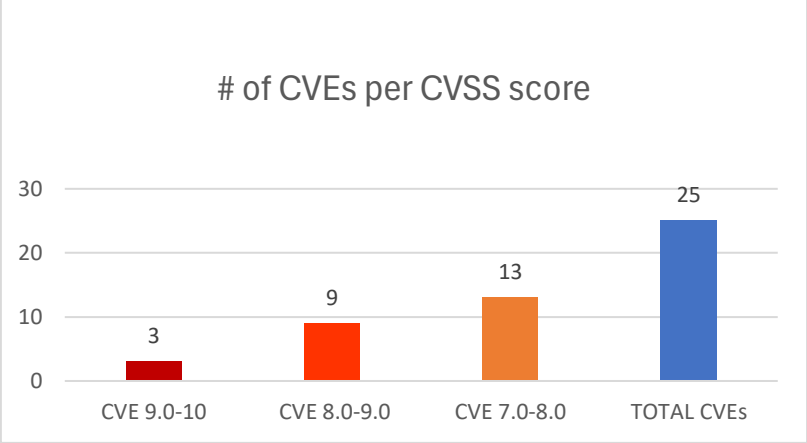
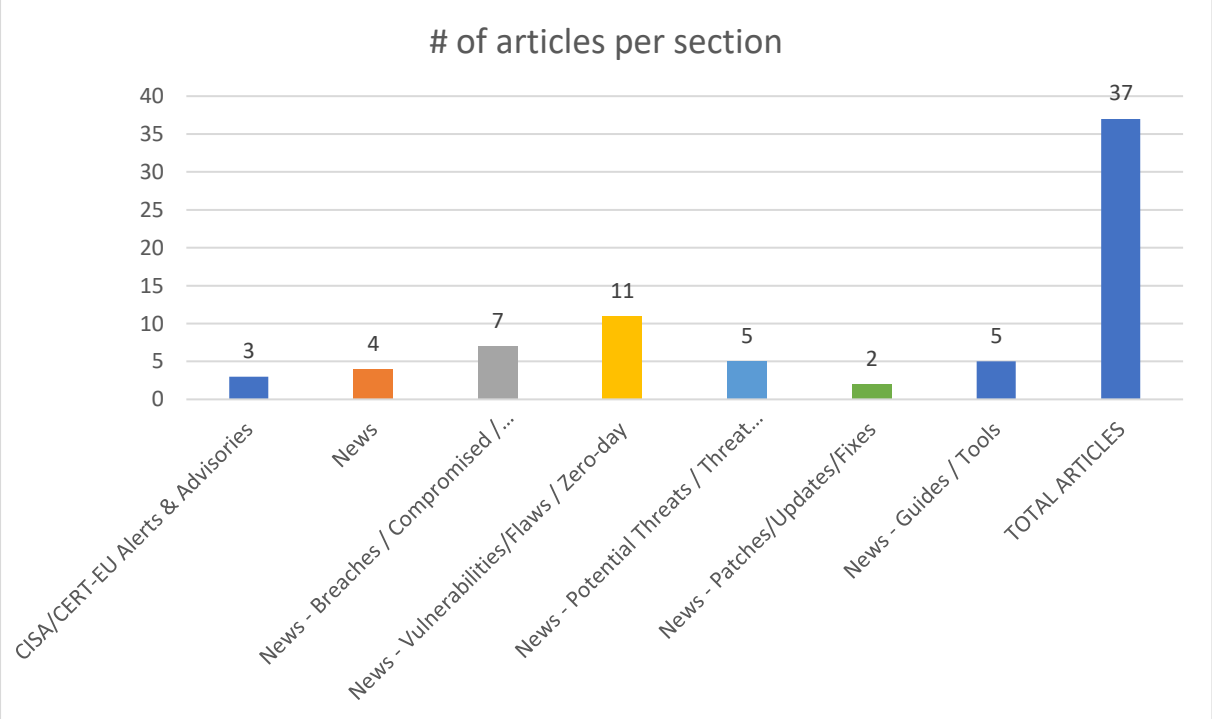
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 17/09/2025 - 19/09/2025





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-2025-10439	9,8	Yordam Informatics	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	from 21.5 & 21.6 before 21.7.	https://www.usom.gov.tr/bildirim/tr-25-0268
https://nvd.nist.gov/vuln/detail/CVE-2025-5948	9,8	The Service Finder Bookings plugin for WordPress	Authorization Bypass Through User-Controlled Key	all versions up to, and including, 6.0	https://themeforest.net/item/service-finder-service-and-business-listing-wordpress-theme/15208793 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/7eb018bc-2650-4e0d-8da9-325eac826d45?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-9972	9,3	The N-Reporter, N-Cloud, and N-Probe	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')		https://www.planet.com.tw/en/support/security-advisory/8 TWCERT/CC https://www.twcert.org.tw/en/cp-139-10390-7ce12-2.html TWCERT/CC https://www.twcert.org.tw/tw/cp-132-10389-265a3-1.html
https://nvd.nist.gov/vuln/detail/CVE-2025-10205	8,8	ABB FLXEON	Use of a One-Way Hash without a Salt	through 9.3.5. and newer versions	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108471A7121&LanguageCode=en&DocumentPartId=pdf&Action=Launch

https://nvd.nist.gov/vuln/detail/CVE-2025-10057	8,8	The WP Import – Ultimate CSV XML Importer for WordPress plugin for WordPress	Improper Control of Generation of Code ('Code Injection')	all versions up to, and including, 7.28	https://plugins.trac.wordpress.org/browser/wp-ultimate-csv-importer/tags/7.25/importExtensions/ImportHelpers.php#L585 Wordfence https://plugins.trac.wordpress.org/changeset/3360428/wp-ultimate-csv-importer/trunk/importExtensions/ImportHelpers.php Wordfence https://plugins.trac.wordpress.org/changeset/3360428/wp-ultimate-csv-importer/trunk/uploadModules/DesktopUpload.php Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/925af22b-a728-496e-a63a-5966347ebe6c?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-9216	8,8	he StoreEngine – Powerful WordPress eCommerce Plugin for Payments, Memberships, Affiliates, Sales & More plugin for WordPress	Unrestricted Upload of File with Dangerous Type	all versions up to, and including, 1.5.0	https://github.com/d0n601/CVE-2025-9216 Wordfence https://plugins.trac.wordpress.org/browser/storeengine/trunk/addons/csv/ajax/import.php#L52 Wordfence https://plugins.trac.wordpress.org/changeset/3360097/storeengine/trunk/addons/csv/ajax/import.php Wordfence https://ryankozak.com/posts/cve-2025-9216/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/7f8cc393-4d6f-4d15-ad95-d4a89dfe433c?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-59458	8,3	JetBrains Junie	Improper Neutralization of Special Elements used in a Command ('Command Injection')	before 252.284.66, 251.284.66, 243.284.66, 252.284.61, 251.284.61, 243.284.61, 252.284.50, 252.284.54, 251.284.54, 251.284.50, 243.284.54, 243.284.50	https://www.jetbrains.com/privacy-security/issues-fixed/
https://nvd.nist.gov/vuln/detail/CVE-2025-55068	8,2	Dover Fueling Solutions ProGauge MagLink LX4 Devices	Integer Overflow or Wraparound		https://www.cisa.gov/news-events/ics-advisories/icsa-25-261-07 ICS-CERT

					https://www.doverfuelingsolutions.com/mea/en/products-and-solutions/automatic-tank-gauging/consoles/progauge-maglink-lx-4-console.html
https://nvd.nist.gov/vuln/detail/CVE-2025-5955	8,1	The Service Finder SMS System plugin for WordPress	Authentication Bypass Using an Alternate Path or Channel	all versions up to, and including, 2.0.0	https://themeforest.net/item/service-finder-service-and-business-listing-wordpress-theme/15208793 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/cc4598a7-d5cf-4553-b29a-659fe288ece9?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-8565	8,1	The Privacy Policy Generator, Terms & Conditions Generator WordPress Plugin : WP Legal Pages plugin for WordPress	Missing Authorization	all versions up to, and including, 3.4.3	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3355766%40wplegal-pages%2Ftrunk&old=3348524%40wplegal-pages%2Ftrunk&sfp_email=&sfph_mail= Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/ed5f2c6d-a548-44c1-a07a-e33999bb164d?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-44034	8,0	oa_system oasys	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	v.1.1	https://github.com/qkdjksfkeg/Security-Collections/blob/main/sqlinjection2.md
https://nvd.nist.gov/vuln/detail/CVE-2025-59518	8,0	LemonLDAP::NG	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'	before 2.16.7 and 2.17 through 2.21 before 2.21.3	https://gitlab.ow2.org/lemonldap-ng/lemonldap-ng/-/commit/228d01945d48015f3f9ea8a8dc64d7e6a27750e9 MITRE https://gitlab.ow2.org/lemonldap-ng/lemonldap-ng/issues/3462
https://nvd.nist.gov/vuln/detail/CVE-2025-9450	7,8	SOLIDWORKS eDrawings	Use of Uninitialized Variable		https://www.3ds.com/trust-center/security/security-advisories/cve-2025-9450
https://nvd.nist.gov/vuln/detail/CVE-2025-50255	7,8	Smartvista BackOffice SmartVista Suite	Cross-Site Request Forgery (CSRF)	2.2.22	https://gitlab.com/c2at3/cve-2025-50255/-/blob/main/Bypassing_CSRF_Protection_in_Smartvista-BackOffice.pdf
https://nvd.nist.gov/vuln/detail/CVE-2025-54860	7,7	Cognex In-Sight Explorer and In-	Improper Restriction of Excessive Authentication Attempts		https://www.cisa.gov/news-events/ics-advisories/icsa-25-261-06

		Sight Camera Firmware			
https://nvd.nist.gov/vuln/detail/CVE-2025-7403	7,6	bt_conn_tx_processor	Write-what-where Condition		https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-9r46-cqqw-6j2j
https://nvd.nist.gov/vuln/detail/CVE-2025-41248	7,5	The Spring Security	Authentication Bypass by Alternate Name		https://spring.io/security/cve-2025-41248
https://nvd.nist.gov/vuln/detail/CVE-2025-10143	7,5	The Catch Dark Mode plugin for WordPress	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion	all versions up to, and including, 2.0	https://plugins.trac.wordpress.org/browser/catch-dark-mode/trunk/plugin.php#L483 Wordfence https://plugins.trac.wordpress.org/changeset/3359058/ Wordfence https://wordpress.org/plugins/catch-dark-mode Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/46776cd5-5262-46ea-b56c-0cbf2b9ae43d?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-59424	7,3	LinkAce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Prior to 2.3.1	https://github.com/Kovah/LinkAce/commit/c0d21b974b32f1ca2fab550fb476c573a068e196 GitHub, Inc. https://github.com/Kovah/LinkAce/security/advisories/GHSA-289g-9gff-p4wh
https://nvd.nist.gov/vuln/detail/CVE-2025-55912	7,3	ClipBucket	Unrestricted Upload of File with Dangerous Type	5.5.0 and prior versions	https://github.com/MacWarrior/clipbucket-v5/blob/5.5.0/upload/actions/photo_uploader.php MITRE https://github.com/MacWarrior/clipbucket-v5/releases?page=2 MITRE https://github.com/MacWarrior/clipbucket-v5/tree/5.5.0 MITRE https://medium.com/@mukund.s1337/cve-2025-55912-clipbucket-5-5-0-unauthenticated-arbitrary-file-upload-rce-720c0c0fbc58
https://nvd.nist.gov/vuln/detail/CVE-2025-37127	7,2	HPE Aruba Networking Edge-Connect SD-WAN Gateways			https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04943en_us&docLocale=en_US

https://nvd.nist.gov/vuln/detail/CVE-2025-58116	7,2	WN-7D36QR and WN-7D36QR/UE	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')		https://jvn.jp/en/vu/JVNVU97490987/ JPCERT/CC https://www.iodata.jp/support/information/2025/09_wn-7d36qr/index.htm
https://nvd.nist.gov/vuln/detail/CVE-2025-8411	7,1	Dokuzsoft Technology E-Commerce Web Design Product	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	before 11.08.2025	https://www.usom.gov.tr/bildirim/tr-25-0267
https://nvd.nist.gov/vuln/detail/CVE-2025-10456	7,1	Bluetooth Low Energy (BLE) fixed channels (such as SMP or ATT)	Integer Overflow or Wraparound	Integer Overflow or Wraparound	https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-hcc8-3qr7-c9m8
https://nvd.nist.gov/vuln/detail/CVE-2025-59215	7,0	Microsoft Graphics Component	Use After Free		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59215

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.

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Releases Eight Industrial Control Systems Advisories	▪ **ICSA-25-259-01 Schneider Electric Altivar Products, ATVdPAC Module, ILC992 InterLink Converter** ▪ **ICSA-25-259-02 Hitachi Energy RTU500 Series** ▪ **ICSA-25-259-03 Siemens SIMATIC NET CP, SINEMA, and SCALANCE** ▪ **ICSA-25-259-04 Siemens RUGGEDCOM, SINEC NMS, and SINEMA** ▪ **ICSA-25-259-05 Siemens OpenSSL Vulnerability in Industrial Products** ▪ **ICSA-25-259-06 Siemens Multiple Industrial Products** ▪ **ICSA-25-259-07 Delta Electronics DIALink** ▪ **ICSA-25-140-07 Schneider Electric Galaxy VS, Galaxy VL, Galaxy VXL (Update A)**	**https://www.cisa.gov/news-events/alerts/2025/09/16/cisa-releases-eight-industrial-control-systems-advisories**
CISA Releases Malware Analysis Report on Malicious Listener Targeting Ivanti Endpoint Manager Mobile Systems	**CVE-2025-4427 and CVE-2025-4428**	https://www.cisa.gov/news-events/alerts/2025/09/18/cisa-releases-malware-analysis-report-malicious-listener-targeting-ivanti-endpoint-manager-mobile
CISA Releases Nine Industrial Control Systems Advisories	▪ **ICSA-25-261-01 Westermo Network Technologies WeOS 5** ▪ **ICSA-25-261-02 Westermo Network Technologies WeOS 5** ▪ **ICSA-25-261-03 Schneider Electric Saitel DR & Saitel DP Remote Terminal Unit** ▪ **ICSA-25-261-04 Hitachi Energy Asset Suite** ▪ **ICSA-25-261-05 Hitachi Energy Service Suite** ▪ **ICSA-25-261-06 Cognex In-Sight Explorer and In-Sight Camera Firmware** ▪ **ICSA-25-261-07 Dover Fueling Solutions ProGauge MagLink LX4 Devices** ▪ **ICSA-25-191-10 End-of-Train and Head-of-Train Remote Linking Protocol (Update C)** ▪ **ICSA-24-030-02 Mitsubishi Electric FA Engineering Software Products (Update D)**	https://www.cisa.gov/news-events/alerts/2025/09/18/cisa-releases-nine-industrial-control-systems-advisories

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.

News

Σύντομη περιγραφή / Τίτλος	URL
North Korean Group Targets South With Military ID Deepfakes	https://www.darkreading.com/cyberattacks-data-breaches/north-korean-group-south-military-id-deepfakes
TikTok Deal Won't End Enterprise Risks	https://www.darkreading.com/cyber-risk/tiktok-deal-enterprise-risks
Microsoft Disrupts 'RaccoonO365' Phishing Service	https://www.darkreading.com/application-security/microsoft-disrupts-raccoono365-phishing-service
China-Aligned TA415 Hackers Uses Google Sheets and Google Calendar for C2 Communications	https://cybersecuritynews.com/china-aligned-ta415-hackers-uses-google-sheets/

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.

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Massive “Shai-Halud” Supply Chain Attack Compromised 477 NPM Packages	https://cybersecuritynews.com/shai-halud-supply-chain-attack/
FinWise Insider Breach Exposes 700K Customer Records to Former Employee	https://cybersecuritynews.com/finwise-insider-breach/
New York Blood Center notifies 194,000 people of data breach	https://www.comparitech.com/news/new-york-blood-center-notifies-194000-people-of-data-breach/?&web_view=true
VC giant Insight Partners warns thousands after ransomware breach	https://www.bleepingcomputer.com/news/security/vc-giant-insight-partners-warns-thousands-after-ransomware-breach/?&web_view=true
Attack on SonicWall’s cloud portal exposes customers’ firewall configurations	https://cyberscoop.com/sonicwall-cyberattack-customer-firewall-configurations/?&web_view=true
BMW Allegedly Breached by Everest Ransomware Group, Internal Documents Reportedly Stolen	https://cybersecuritynews.com/bmw-allegedly-breached/
1 in 3 Android Apps Leak Sensitive Data	https://www.infosecurity-magazine.com/news/android-apps-leak-sensitive-data/

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.

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Linux Kernel's KSMBD Subsystem Vulnerability Let Remote Attackers Exhaust Server Resources	**https://cybersecuritynews.com/linux-kernels-ksmbd-subsystem-vulnerability/**
Hackers Can Exploit Bitpixie Vulnerability to Bypass BitLocker Encryption and Escalate Privileges	**https://cybersecuritynews.com/bitpixie-vulnerability-bypass-bitlocker/**
0-Click ChatGPT Agent Vulnerability Allows Sensitive Data Exfiltration from Gmail	**https://cybersecuritynews.com/0-click-chatgpt-agent-vulnerability/**
PureVPN Vulnerability Exposes Users IPv6 Address While Toggling Wi-Fi	**https://cybersecuritynews.com/purevpn-vulnerability/**
How a Plaintext File On Users' Desktops Exposed Secrets Leads to Akira Ransomware Attacks	**https://cybersecuritynews.com/plaintext-file-exposed-secrets/**
CISA Warns of Two Malware Strains Exploiting Ivanti EPMM CVE-2025-4427 and CVE-2025-4428	https://thehackernews.com/2025/09/cisa-warns-of-two-malware-strains.html
Unpatched Vulnerabilities Expose Novakon HMIs to Remote Hacking	https://www.securityweek.com/unpatched-vulnerabilities-expose-novakon-hmis-to-remote-hacking/
Pixie Dust Wi-Fi Attack Exploits Routers WPS to Obtain PIN and Connect With Wireless Network	https://cybersecuritynews.com/pixie-dust-wi-fi-attack/
Critical Microsoft's Entra ID Vulnerability Allows Attackers to Gain Complete Administrative Control	https://cybersecuritynews.com/microsofts-entra-id-vulnerability/
TP-Link Router 0-Day RCE Vulnerability Exploited Bypassing ASLR Protections – PoC Released	https://cybersecuritynews.com/tp-link-router-zero-day-rce-vulnerability/
WatchGuard warns of critical vulnerability in Firebox firewalls	https://www.bleepingcomputer.com/news/security/watchguard-warns-of-critical-vulnerability-in-firebox-firewalls/

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.

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Google Patches Chrome Zero-Day CVE-2025-10585 as Active V8 Exploit Threatens Millions	https://thehackernews.com/2025/09/google-patches-chrome-zero-day-cve-2025.html
Jenkins Patches Multiple Vulnerabilities that Allow Attackers to Cause a Denial of Service	https://cybersecuritynews.com/jenkins-patches-multiple-vulnerabilities/

Η συγκεκριμένη ενότητα ασχολείται με νέες απειλές, εξελιγμένα malware και τεχνικές επιθέσεων που έχουν εντοπιστεί σε πραγματικές συνθήκες. Περιλαμβάνονται αναφορές σε εργαλεία που χρησιμοποιούν οι επιτιθέμενοι, αλλά και δείκτες (IoCs) που μπορούν να χρησιμοποιηθούν στην άμυνα.

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Raven Stealer Scavenges Chromium Data Via Telegram	https://www.darkreading.com/vulnerabilities-threats/raven-stealer-scavenges-chrome-data-telegram
New Phishing Attack Targets Facebook Users to Steal Login Credentials	https://cybersecuritynews.com/new-phishing-attack-targets-facebook-users/
New iOS Video Injection Tool Bypasses Biometric Verification with Jailbroken iPhones	https://cybersecuritynews.com/biometric-verification-with-jailbroken-iphones/
Hackers Injecting Malicious Code into GitHub Actions Workflows to Steal PyPI Publishing Tokens	https://cybersecuritynews.com/github-actions-workflows-to-steal-pypi/
New ‘shinysp1d3r’ Ransomware-as-a-service in Active Development to Encrypt VMware ESXi Environments	https://cybersecuritynews.com/new-shinysp1d3r-ransomware-as-a-service-in-active-development/

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.

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Top Tools for Enterprise Security Monitoring	**https://cybersecuritynews.com/enterprise-security-monitoring-tools/**
10 Best Vulnerability Management Tools In 2025	https://cybersecuritynews.com/vulnerability-management-tools/
Splunk Releases Guide to Detect Remote Employment Fraud Within Your Organization	https://cybersecuritynews.com/detect-remote-employment-fraud/
Top 15 Best Security Incident Response Tools In 2025	https://cybersecuritynews.com/incident-response-tools/
10 Best API Protection Tools in 2025	https://cybersecuritynews.com/best-api-protection-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/