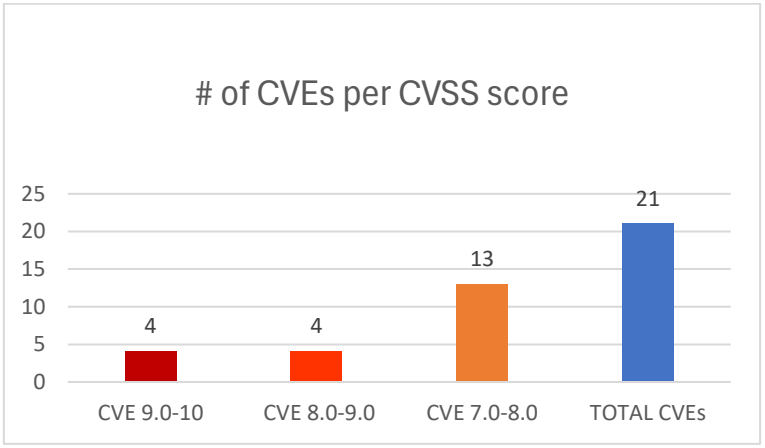
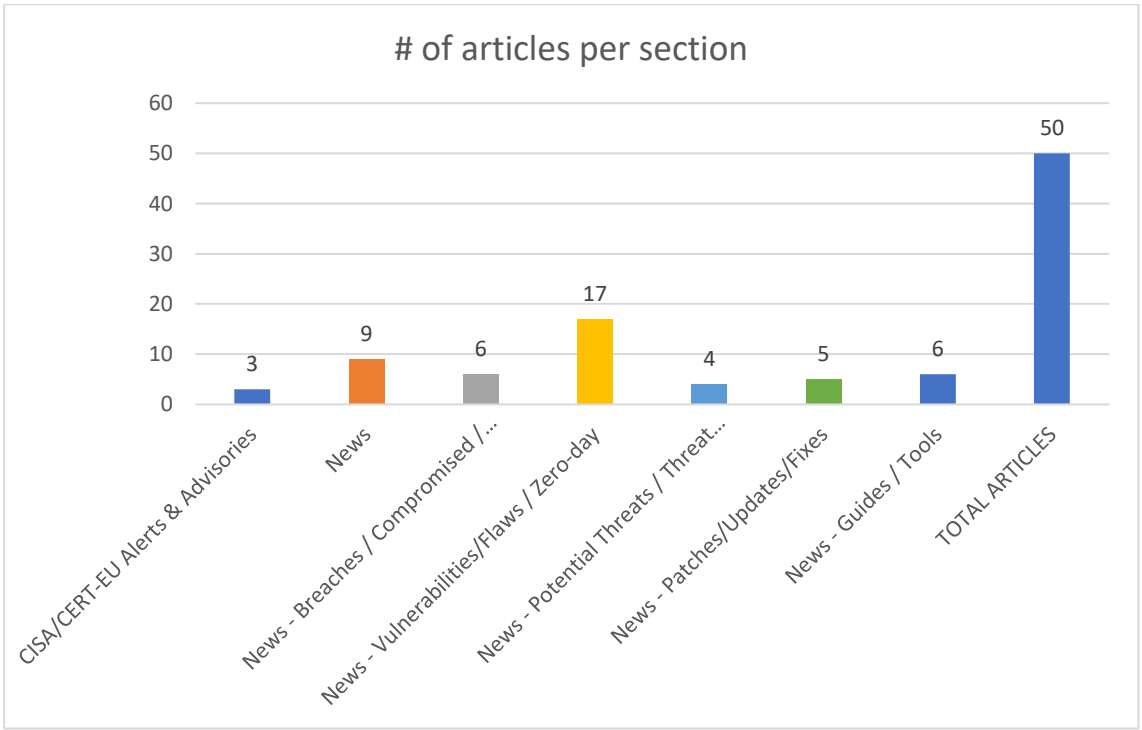
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 15/10/2025 - 17/10/2025





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-2025-10041]	9,8	The Flex QR Code Generator plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 1.2.5	https://plugins.trac.wordpress.org/browser/flex-qr-code-generator/tags/1.2.5/qr-code-generator.php#L208 Wordfence https://wordpress.org/plugins/flex-qr-code-generator/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/40000879-a5ef-48f2-97e4-77d527259af0?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-10294	9,8	The OwnID Passwordless Login plugin for WordPress	Authentication Bypass Using an Alternate Path or Channel	up to, and including, 1.3.4	https://wordpress.org/plugins/ownid-passwordless-login/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/b8dd6008-e9b8-4a87-b1c7-0dc272850cbd?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-9967	9,8	The Orion SMS OTP Verification plugin for WordPress	Authentication Bypass Using an Alternate Path or Channel	up to, and including, 1.1.7	https://plugins.trac.wordpress.org/browser/orion-sms-otp-verification/trunk/vendor/js/reset-password.js Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/b121fdb4-93a8-400c-89c2-3195cb40e03c?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-10294	9,8	The OwnID Passwordless Login plugin for WordPress	Authentication Bypass Using an Alternate Path or Channel	up to, and including, 1.3.4.	https://wordpress.org/plugins/ownid-passwordless-login/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/b8dd6008-e9b8-4a87-b1c7-0dc272850cbd?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-11746	8,8	The XStore theme for WordPress	Improper Limitation of a Pathname to a	up to, and including, 9.5.4	https://www.wordfence.com/threat-intel/vulnerabilities/id/2a49db7f-62fc-472d-9edf-de5edbe48219?source=cve Wordfence https://xstore.8theme.com/update-history/

			Restricted Directory ('Path Traversal')		
https://nvd.nist.gov/vuln/detail/CVE-2025-10293	8,8	The Keyy Two Factor Authentication (like Clef) plugin for WordPress	Improper Authentication	up to, and including, 1.2.3	https://wordpress.org/plugins/keyy/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/1850e6bd-04bc-4510-aba9-e51431363231?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-10299	8,8	The WPBifröst – Instant Passwordless Temporary Login Links plugin for WordPress	Missing Authorization	up to, and including, 1.0.7	https://wordpress.org/plugins/create-temporary-login/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/50946bc7-8d31-4376-bdcc-de7aad700503?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-54263	8,1	Adobe Commerce	Incorrect Authorization	2.4.9-alpha2, 2.4.8-p2, 2.4.7-p7, 2.4.6-p12, 2.4.5-p14, 2.4.4-p15	https://helpx.adobe.com/security/products/magento/apsb25-94.html
https://nvd.nist.gov/vuln/detail/CVE-2025-54279	7,8	Animate	Use After Free	23.0.13, 24.0.10 and earlier	https://helpx.adobe.com/security/products/animate/apsb25-97.html
https://nvd.nist.gov/vuln/detail/CVE-2025-54268	7,8	Bridge	Heap-based Buffer Overflow	14.1.8, 15.1.1	https://helpx.adobe.com/security/products/bridge/apsb25-96.html
https://nvd.nist.gov/vuln/detail/CVE-2025-26861	7,8	RemoteCall Remote Support Program (for Operator)	Uncontrolled Search Path Element	prior to 5.3.0	https://jvn.jp/en/jp/JVN22713803/ JPCERT/CC https://www.remotecall.com/en/support/download/

https://nvd.nist.gov/vuln/detail/CVE-2025-26859	7,8	RemoteView PC Application Console	Uncontrolled Search Path Element	prior to 6.0.2	https://help.rview.com/hc/en-us/articles/4420613945875-Notice-of-termination-of-RemoteView-PC-application-console-service JPCERT/CC https://jvn.jp/en/jp/JVN22713803/
https://nvd.nist.gov/vuln/detail/CVE-2025-11501	7,5	The Dynamically Display Posts plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to, and including, 1.1	https://plugins.trac.wordpress.org/browser/dynamically-display-posts/trunk/includes/frontend/classes/database-talk.php#L38 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/b2ad5698-4299-48a4-bcc1-5f4436dfab27?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-11722	7,5	The Woocommerce Category and Products Accordion Panel plugin for WordPress	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusio	up to, and including, 1.0	https://plugins.trac.wordpress.org/browser/accordion-panel-for-category-and-products/tags/1.0/include/abstract.php#L256 Wordfence https://plugins.trac.wordpress.org/browser/accordion-panel-for-category-and-products/tags/1.0/include/categoryaccordionpanel.php#L87 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/55315ba1-cbb8-4ce1-96c6-30a02611ba47?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-11177	7,5	The External Login plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to, and including, 1.11.2	https://plugins.trac.wordpress.org/browser/external-login/tags/1.11.2/login/db.php#L153 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/488f1a2f-01c8-40cf-b52f-d707271105f5?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-10743	7,5	The Outdoor plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to, and including, 1.3.2	https://plugins.trac.wordpress.org/browser/outdoor/trunk/actions.php#L73 Wordfence https://wordpress.org/plugins/outdoor/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/6038accc-98ac-496c-9c53-ec06b2045324?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-6042	7,3	The Lisfinity Core - Lisfinity Core plugin used for pebas® Lisfinity WordPress	Improper Privilege Management	up to, and including, 1.4.0	https://themeforest.net/item/lisfinity-classified-ads-wordpress-theme/26342611 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/afffd5e2-798b-42b5-b0b9-ac7d6d06edbb?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-61941	7,2	WXR9300BE6P series firmware	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	prior to Ver.1.10.	https://jvn.jp/en/vu/JVNVU96471278/ JPCERT/CC https://www.buffalo.jp/news/detail/20251014-01.html
https://nvd.nist.gov/vuln/detail/CVE-2025-10051	7,2	The Demo Import Kit plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 1.1.0	https://wordpress.org/plugins/demo-import-kit/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/465f2fd1-9eb3-43ca-8acc-74acf6bcde1a?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-10754	7,2	The DocoDoco Store Locator plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 1.0.1	https://plugins.trac.wordpress.org/browser/docodoco-store-locator/tags/1.0.1/includes/Admin/ZIP.php#L187 Wordfence https://plugins.trac.wordpress.org/browser/docodoco-store-locator/tags/1.0.1/includes/Admin/ZIP.php#L275 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/14759eb0-455f-4b7d-abab-4e4d89b32bb1?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-10313	7,2	The Find And Replace content for WordPress plugin	Missing Authorization	up to, and including, 1.1	https://plugins.trac.wordpress.org/browser/find-and-replace-content/trunk/function.php?rev=1601465 Wordfence https://wordpress.org/plugins/find-and-replace-content/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/c0469ece-6f5f-4774-8094-f7f67702a775?source=cve

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 Releases Thirteen Industrial Control Systems Advisories	▪ **ICSA-25-289-01** Rockwell Automation FactoryTalk View Machine Edition and PanelView Plus 7 ▪ **ICSA-25-289-02** Rockwell Automation FactoryTalk Linx ▪ **ICSA-25-289-03** Rockwell Automation FactoryTalk ViewPoint ▪ **ICSA-25-289-04** Rockwell Automation ArmorStart AOP ▪ **ICSA-25-289-05** Siemens Solid Edge ▪ **ICSA-25-289-06** Siemens SiPass Integrated ▪ **ICSA-25-289-07** Siemens SIMATIC ET 200SP Communication Processors ▪ **ICSA-25-289-08** Siemens SINEC NMS ▪ **ICSA-25-289-09** Siemens TeleControl Server Basic ▪ **ICSA-25-289-10** Siemens HyperLynx and Industrial Edge App Publisher ▪ **ICSA-25-289-11** Hitachi Energy MACH GWS ▪ **ICSA-25-224-03** Schneider Electric EcoStruxure (Update A) ▪ **ICSA-24-121-01** Delta Electronics CNCSoft-G2 DOPSoft (Update A)	https://www.cisa.gov/news-events/alerts/2025/10/16/cisa-releases-thirteen-industrial-control-systems-advisories
CISA Directs Federal Agencies to Mitigate Vulnerabilities in F5 Devices		https://www.cisa.gov/news-events/alerts/2025/10/15/cisa-directs-federal-agencies-mitigate-vulnerabilities-f5-devices
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2025-54253 **Adobe Experience Manager Forms Code Execution Vulnerability**	https://www.cisa.gov/news-events/alerts/2025/10/15/cisa-adds-one-known-exploited-vulnerability-catalog

News

Η ενότητα "News" συνοψίζει τα πιο σημαντικά γεγονότα της εβδομάδας στον τομέα της κυβερνοασφάλειας. Εδώ θα βρείτε επιθέσεις που ξεχώρισαν, νέες τεχνικές που εντοπίστηκαν, ή ενέργειες από γνωστές ομάδες hacking. Δίνει την απαραίτητη εικόνα του τι συμβαίνει διεθνώς και πού πρέπει να στραφεί η προσοχή.

Σύντομη περιγραφή / Τίτλος	URL
AISLE Emerges From Stealth With AI-Based Reasoning System to Remediate Vulnerabilities on the Fly	https://www.securityweek.com/aisle-emerges-from-stealth-with-ai-based-reasoning-system-that-remediates-vulnerabilities-on-the-fly/
China Hackers Test AI-Optimized Attack Chains in Taiwan	https://www.darkreading.com/threat-intelligence/china-hackers-ai-optimized-attack-taiwan
Africa Remains Top Global Target, Even as Attacks Decline	https://www.darkreading.com/cyber-risk/africa-top-global-target-attacks-decline
Leaks in Microsoft VS Code Marketplace Put Supply Chain at Risk	https://www.darkreading.com/application-security/leaks-microsoft-vs-code-marketplaces-supply-chain-risks
Capita Fined £14m After 2023 Breach that Hit 6.6 Million People	https://www.infosecurity-magazine.com/news/capita-fined-14m-2023-breach-66/
Whisper 2FA Behind One Million Phishing Attempts Since July	https://www.infosecurity-magazine.com/news/whisper-2fa-behind-1m-phishing/
AI Attacks Surge as Microsoft Process 100 Trillion Signals Daily	https://www.infosecurity-magazine.com/news/microsoft-process-100-trillion/
New nightMARE Python Library to Analyze Malware and Extract Intelligence Indicators	https://cybersecuritynews.com/new-nightmare-python-library-to-analyze-malware/
Pro-Russian Hacktivist Group Attacking Government Portals, Financial Services and Online Commerce	https://cybersecuritynews.com/pro-russian-hacktivist-group-attacking-government-portals/

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
F5 Breach Exposes BIG-IP Source Code — Nation-State Hackers Behind Massive Intrusion	https://thehackernews.com/2025/10/f5-breach-exposes-big-ip-source-code.html
Harvard University Breached in Oracle Zero-Day Attack	https://www.darkreading.com/cyberattacks-data-breaches/harvard-breached-oracle-zero-day-attack
Flaw in Slider Revolution Plugin Exposed 4m WordPress Sites	https://www.infosecurity-magazine.com/news/flaw-slider-revolution-plugin/
Over 23 Million Victims Hit by Data Breaches in Q3	https://www.infosecurity-magazine.com/news/over-23-million-victims-data/
178K Invoicely Records Exposed in Cloud Data Leak	https://www.esecurityplanet.com/news/invoicely-178k-records-cloud-misconfiguration/?&web_view=true

BlackSuit Ransomware Actors Breached Corporate Environment, Including 60+ VMware ESXi Hosts	https://cybersecuritynews.com/blacksuit-ransomware-vmware-esxi/

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
New SAP NetWeaver Bug Lets Attackers Take Over Servers Without Login	https://thehackernews.com/2025/10/new-sap-netweaver-bug-lets-attackers.html
Hackers Target ICTBroadcast Servers via Cookie Exploit to Gain Remote Shell Access	https://thehackernews.com/2025/10/hackers-target-ictbroadcast-servers-via.html
Two CVSS 10.0 Bugs in Red Lion RTUs Could Hand Hackers Full Industrial Control	https://thehackernews.com/2025/10/two-cvss-100-bugs-in-red-lion-rtus.html
Two New Windows Zero-Days Exploited in the Wild — One Affects Every Version Ever Shipped	https://thehackernews.com/2025/10/two-new-windows-zero-days-exploited-in.html
LinkPro Linux Rootkit Uses eBPF to Hide and Activates via Magic TCP Packets	https://thehackernews.com/2025/10/linkpro-linux-rootkit-uses-ebpf-to-hide.html
Hackers Deploy Linux Rootkits via Cisco SNMP Flaw in 'Zero Disco' Attacks	https://thehackernews.com/2025/10/hackers-deploy-linux-rootkits-via-cisco.html
CISA Flags Adobe AEM Flaw with Perfect 10.0 Score — Already Under Active Attack	https://thehackernews.com/2025/10/cisa-flags-adobe-aem-flaw-with-perfect.html
Senate Investigates Cisco Over Zero-Day Firewall Vulnerabilities	https://cybersecuritynews.com/senate-cisco-zero-day-vulnerabilities/
CISA Warns Of Windows Improper Access Control Vulnerability Exploited In Attacks	https://cybersecuritynews.com/windows-improper-access-control-vulnerability/
Critical Apache ActiveMQ Vulnerability Let Attackers Execute Arbitrary Code	https://cybersecuritynews.com/apache-activemq-vulnerability-3/
Critical Samba RCE Vulnerability Enables Arbitrary Code Execution	https://cybersecuritynews.com/critical-samba-rce-vulnerability/
Windows BitLocker Vulnerabilities Let Attackers Bypass Security Feature	https://cybersecuritynews.com/windows-bitlocker-vulnerabilities/
Microsoft Disrupted Vanilla Tempest Attack by Revoking Certificates Used to Sign Fake Teams File	https://cybersecuritynews.com/vanilla-tempest-fake-teams-file/
Windows Agere Modem Driver 0-Day Vulnerabilities Actively Exploited To Escalate Privileges	https://cybersecuritynews.com/windows-agere-modem-driver-0-day/
CISA Warns Of Rapid7 Velociraptor Vulnerability Exploited in Ransomware Attacks	https://cybersecuritynews.com/cisa-rapid7-velociraptor-vulnerability/
Critical Veeam Backup RCE Vulnerabilities Let Attackers Execute Malicious Code Remotely	https://cybersecuritynews.com/veeam-backup-rce-vulnerabilities/
Chrome Use After Free Vulnerability Let Attackers Execute Arbitrary Code	https://cybersecuritynews.com/google-chrome-use-after-free-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
High-Severity Vulnerabilities Patched by Fortinet and Ivanti	https://www.securityweek.com/high-severity-vulnerabilities-patched-by-fortinet-and-ivanti/
Adobe Patches Critical Vulnerability in Connect Collaboration Suite	https://www.securityweek.com/adobe-patches-critical-vulnerability-in-collaboration-suite/
Gladinet fixes actively exploited zero-day in file-sharing software	https://www.bleepingcomputer.com/news/security/gladinet-fixes-actively-exploited-zero-day-in-file-sharing-software/
Last Windows 10 Patch Tuesday Features Six Zero-Days	https://www.infosecurity-magazine.com/news/last-windows-10-patch-tuesday-six/
Microsoft Security Update Causes Active Directory Sync Failures on Windows Server 2025	https://cybersecuritynews.com/microsoft-update-active-directory-sync/

Potential threats / Threat intelligence

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.

Σύντομη περιγραφή / Τίτλος	URL
North Korean Hackers Using Malicious Scripts Combining BeaverTail and Otter-Cookie for Keylogging	https://cybersecuritynews.com/north-korean-hackers-using-malicious-scripts-combining-beavertail-and-ottercookie-for-keylogging/
Operation Silk Lure Weaponizing Windows Scheduled Tasks to Drop ValleyRAT	https://cybersecuritynews.com/operation-silk-lure-weaponizing-windows-scheduled-tasks/
Qilin Ransomware Using Ghost Bulletproof Hosting to Attack Organizations Worldwide	https://cybersecuritynews.com/qilin-ransomware-using-ghost-bulletproof-hosting/
New Phishing Attack Uses Basic Auth URLs to Trick Users and Steal Login Credentials	https://cybersecuritynews.com/new-phishing-attack-uses-basic-auth-urls/

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/**
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/
ThreatBook Launches Best-of-Breed Advanced Threat Intelligence Solution	https://cybersecuritynews.com/threatbook-advanced-threat-intelligence-solution/

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/