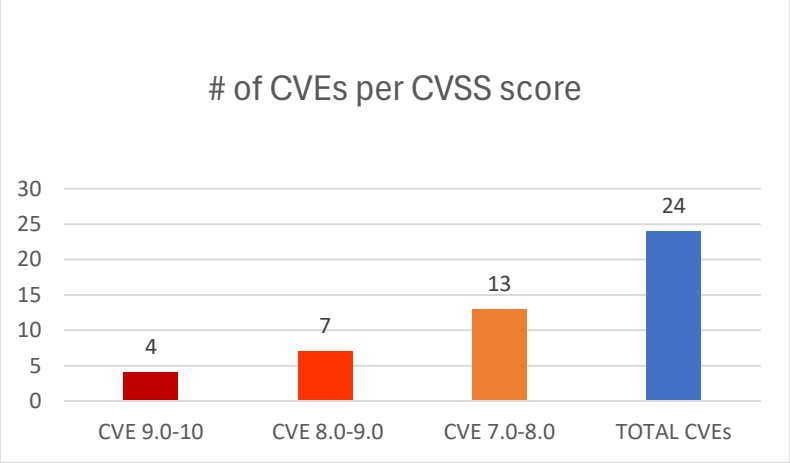
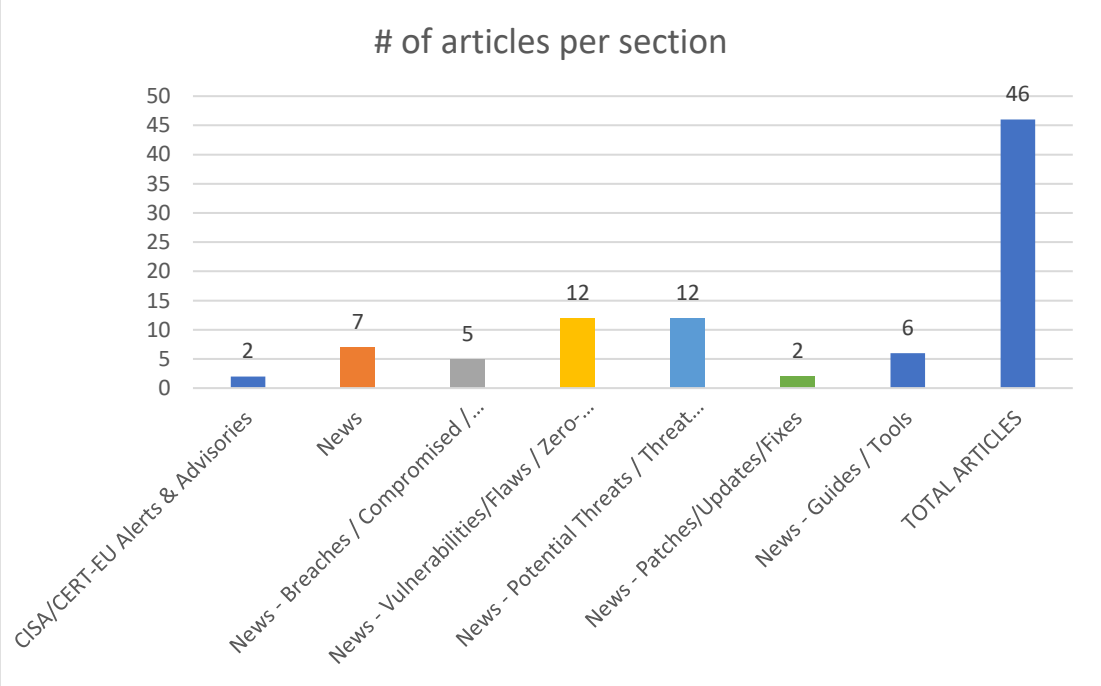
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 08/10/2025 - 10/10/2025





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-2025-11539	9,9	Grafana Image Renderer	Improper Control of Generation of Code ('Code Injection')	from 1.0.0 through 4.0.16	https://github.com/grafana/grafana-image-renderer/releases/tag/v4.0.17 Grafana Labs https://grafana.com/security/security-advisories/cve-2025-11539/
https://nvd.nist.gov/vuln/detail/CVE-2025-59246	9,8	Azure Entra ID Elevation	Missing Authentication for Critical Function		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59246
https://nvd.nist.gov/vuln/detail/CVE-2025-7526	9,8	The WP Travel Engine – Tour Booking Plugin – Tour Operator Software plugin for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	up to, and including, 6.6.7	https://plugins.trac.wordpress.org/browser/wp-travel-engine/tags/6.5.6/includes/dashboard/class-wp-travel-engine-form-handler.php#L512 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/c754d957-26a8-4fef-a487-96d566c2dc36?source=cve
https://blog.blacklanternsecurity.com/p/bbot-security-advisory-gitdumper	9,6	BBOT's gitdumper module	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')		https://blog.blacklanternsecurity.com/p/bbot-security-advisory-gitdumper
https://nvd.nist.gov/vuln/detail/CVE-2025-35055	8,8	Newforma Info Exchange (NIX) '/UserWeb/Common/UploadBlueimp.ashx'	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	before 2023.1	https://raw.githubusercontent.com/cisagov/CSAF/develop/csaf_files/IT/white/2025/va-25-282-01.json Cybersecurity and Infrastructure Security Agency (CISA) U.S. Civilian Government https://www.cve.org/CVERecord?id=CVE-2025-35055 Cybersecurity and Infrastructure Security Agency (CISA) U.S. Civilian Government https://www.cve.org/CVERecord?id=CVE-2025-35062

https://nvd.nist.gov/vuln/detail/CVE-2025-11549	8,8	Tenda W12	Stack-based Buffer Overflow	3.0.0.6(3948)	https://github.com/z472421519/BinaryAudit/blob/main/PoC/BOF/Tenda_W12/cgiWifiMacFilterSet/cgiWifiMacFilterSet.md CISA-ADP, VulDB https://vuldb.com/?ctiid.327708 VulDB https://vuldb.com/?id.327708 VulDB https://vuldb.com/?submit.670110 VulDB https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-11561	8,8	Active Directory and the System Security Services Daemon (SSSD) on Linux systems	Improper Privilege Management		https://access.redhat.com/security/cve/CVE-2025-11561 Red Hat, Inc. https://blog.async.sg/kerberos-ldr Red Hat, Inc. https://bugzilla.redhat.com/show_bug.cgi?id=2402727
https://nvd.nist.gov/vuln/detail/CVE-2025-11526	8,8	Tenda AC7	Stack-based Buffer Overflow	15.03.06.44	https://github.com/noahze01/IoT-vulnerable/blob/main/Tenda/AC7/WifiMacFilterSet.md VulDB Exploit Third Party Advisory https://vuldb.com/?ctiid.327664 VulDB Permissions Required VDB Entry https://vuldb.com/?id.327664 VulDB Third Party Advisory VDB Entry https://vuldb.com/?submit.669854 VulDB Third Party Advisory VDB Entry https://vuldb.com/?submit.669861 VulDB Third Party Advisory VDB Entry https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-59271	8,7	Redis Enterprise Elevation	Improper Authorization		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59271
https://nvd.nist.gov/vuln/detail/CVE-2025-59146	8,5	New API	Server-Side Request Forgery (SSRF)		https://github.com/QuantumNous/new-api/commit/ef634160986c6f6b087cbfe131074fda862928af GitHub, Inc. https://github.com/QuantumNous/new-api/security/advisories/GHSA-xxv6-m6fx-vfhh

https://nvd.nist.gov/vuln/detail/CVE-2025-61773	8,1	pyLoad	Improper Encoding or Escaping of Output	versions prior to 0.5.0b3.dev91	https://github.com/pyload/pyload/commit/5823327d0b797161c7195a1f660266d30a69f0ca GitHub, Inc. https://github.com/pyload/pyload/pull/4624 GitHub, Inc. https://github.com/pyload/pyload/security/advisories/GHSA-cjjf-27cc-pvmv
https://nvd.nist.gov/vuln/detail/CVE-2025-11340	7,7	GitLab	Incorrect Authorization	from 18.3 to 18.3.4, 18.4 to 18.4.2	https://about.gitlab.com/releases/2025/10/08/patch-release-gitlab-18-4-2-released/ GitLab Inc. https://gitlab.com/gitlab-org/gitlab/-/issues/567847
https://nvd.nist.gov/vuln/detail/CVE-2025-59305	7,6	Langfuse	Improper Authorization	3.1 before d67b317	
https://nvd.nist.gov/vuln/detail/CVE-2025-59251	7,6	Microsoft Edge (Chromium-based)	Improper Control of Generation of Code ('Code Injection')		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59251
https://nvd.nist.gov/vuln/detail/CVE-2025-61602	7,5	BigBlueButton	Improper Check or Handling of Exceptional Conditions	versions prior to 3.0.13	https://github.com/bigbluebutton/bigbluebutton/pull/23651 GitHub, Inc. https://github.com/bigbluebutton/bigbluebutton/security/advisories/GHSA-45j2-m26c-3pcm
https://nvd.nist.gov/vuln/detail/CVE-2025-11573	7,5	Amazon.IonDotnet	Improper Validation of Syntactic Correctness of Input	versions <v1.3.2	https://aws.amazon.com/security/security-bulletins/AWS-2025-022/ AMZN https://github.com/amazon-ion/ion-dotnet/releases/tag/v1.3.2 AMZN https://github.com/amazon-ion/ion-dotnet/security/advisories/GHSA-q5r6-9qwq-g2wj
https://nvd.nist.gov/vuln/detail/CVE-2025-60004	7,5	Juniper Networks Junos OS and Junos OS Evolved	Improper Check for Unusual or Exceptional Conditions	Junos OS: * 23.4 versions from 23.4R2-S3 before 23.4R2-S5, * 24.2 versions from 24.2R2 before 24.2R2-S1, * 24.4 versions before 24.4R1-S3, 24.4R2; Junos OS Evolved: * 23.4-EVO versions from 23.4R2-S2-EVO before 23.4R2-S5-EVO, * 24.2-EVO	https://supportportal.juniper.net/JSA103165

				versions from 24.2R2-EVO before 24.2R2-S1-EVO, * 24.4-EVO versions before 24.4R1-S3-EVO, 24.4R2-EVO.	
https://nvd.nist.gov/vuln/detail/CVE-2025-61577	7,5	D-Link DIR-816A2_FW	Stack-based Buffer Overflow	v1.10CNB05	https://github.com/Flechao1/iot-vuln/blob/main/dlink-816-b05.md MITRE https://github.com/peris-navince/founded-0-days/blob/main/Dlink/816/dir_setWanWifi/1.md MITRE https://www.dlink.com/en/security-bulletin/
https://nvd.nist.gov/vuln/detail/CVE-2025-10862	7,5	The Popup builder with Gamification, Multi-Step Popups, Page-Level Targeting, and WooCommerce Triggers plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to, and including, 2.1.3	https://plugins.trac.wordpress.org/browser/popup-builder-block/tags/2.1.2/includes/Helpers/DataBase.php#L374 Wordfence https://plugins.trac.wordpress.org/browser/popup-builder-block/tags/2.1.2/includes/Routes/Popup.php#L232 Wordfence https://plugins.trac.wordpress.org/changeset/3369146/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/93e0a1a1-fba6-4209-b679-e66d77870be2?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-57323	7,5	mpregular	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	version 0.2.0 and before	https://github.com/VulnSageAgent/PoCs/blob/main/JavaScript/prototype-pollution/mpregular%400.2.0/index.js MITRE https://github.com/VulnSageAgent/PoCs/tree/main/JavaScript/prototype-pollution/CVE-2025-57323
https://nvd.nist.gov/vuln/detail/CVE-2025-45095	7,3	Lavasoft Web Companion	Improper Access Control	versions 8.9.0.1091 through 12.1.3.1037	https://gist.github.com/T4rantell/cd73592950c4ac700b40cc8e8e36494d
https://nvd.nist.gov/vuln/detail/CVE-2025-55322	7,3	GitHub	Binding to an Unrestricted IP Address		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-55322

https://nvd.nist.gov/vuln/detail/CVE-2025-10239	7,2	Flowmon	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	prior to 12.5.5	https://community.progress.com/s/article/CVE-2025-10239
https://nvd.nist.gov/vuln/detail/CVE-2025-10496	7,2	The Cookie Notice & Consent plugin for WordPress	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	up to, and including, 1.6.5	https://plugins.trac.wordpress.org/browser/cookie-notice-consent/tags/1.6.5/includes/class-cnc-admin.php#L33 Wordfence https://plugins.trac.wordpress.org/browser/cookie-notice-consent/tags/1.6.5/includes/class-cnc-logger.php#L141 Wordfence https://plugins.trac.wordpress.org/browser/cookie-notice-consent/tags/1.6.5/includes/class-cnc-logger.php#L259 Wordfence https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3373718%40cookie-notice-consent%2Ftrunk&old=3345005%40cookie-notice-consent%2Ftrunk&sfp_email=&sfph_mail= Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/035097dd-8ebd-49b8-93ea-0f957594f130?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 Adds One Known Exploited Vulnerability to Catalog	▪ **CVE-2021-43798 Grafana Path Traversal Vulnerability**	**https://www.cisa.gov/news-events/alerts/2025/10/09/cisa-adds-one-known-exploited-vulnerability-catalog**
CISA Releases Four Industrial Control Systems Advisories	▪ **ICSA-25-282-01 Hitachi Energy Asset Suite** ▪ **ICSA-25-282-02 Rockwell Automation Lifecycle Services with Cisco** ▪ **ICSA-25-282-03 Rockwell Automation Stratix** ▪ **ICSA-25-128-03 Mitsubishi Electric Multiple FA Products (Update A)**	**https://www.cisa.gov/news-events/alerts/2025/10/09/cisa-releases-four-industrial-control-systems-advisories**

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
Pro-Russia Hacktivists “Claim” Attack on Water Utility Honeypot	**https://www.infosecurity-magazine.com/news/russia-hacktivistsattack-water/**
Researchers Warn of Security Gaps in AI Browsers	**https://www.infosecurity-magazine.com/news/architectural-flaws-ai-browsers/**
Bybit Theft Drives Record-Breaking $2bn Haul for North Korea	**https://www.infosecurity-magazine.com/news/bybit-recordbreaking-2bn-north/**
High Number of Windows 10 Users Remain as End-of-Life Looms	**https://www.infosecurity-magazine.com/news/windows-10-users-end-of-life/**
Cyber-Attack Contributes to Huge Sales Drop at JLR	**https://www.infosecurity-magazine.com/news/cyber-attack-sales-drop-jlr/**
OpenAI Banned ChatGPT Accounts Used by Chinese and North Korean Hackers to Develop Malware	**https://cybersecuritynews.com/openai-banned-chatgpt-chinese-accounts/**
77% of Employees Share Company Secrets on ChatGPT Compromising Enterprise Policies	**https://cybersecuritynews.com/employees-share-company-secrets-on-chatgpt/**

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
KFC Venezuela Alleged Data Breach – 1 Million Customer Records Exposed	https://cybersecuritynews.com/kfc-venezuela-alleged-data-breach/
SonicWall Confirms That Hackers Stole All Customers Firewall Configuration Backup Files	https://cybersecuritynews.com/sonicwall-confirms-that-hackers-stole/
Discord Data Breach – 1.5 TB of Data and 2 Million Government ID Photos Extorted	https://cybersecuritynews.com/discord-data-breach-sensitive-data/
Chinese Hackers Breached Law Firm Williams & Connolly via Zero-Day	https://www.securityweek.com/chinese-hackers-breached-law-firm-williams-connolly-via-zero-day/?&web_view=true
Institute of Culinary Education notifies 33,000+ people of data breach that leaked SSNs	https://www.comparitech.com/news/institute-culinary-education-notifies-33000-people-of-data-breach-that-leaked-ssns/?&web_view=true

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
Severe Framelink Figma MCP Vulnerability Lets Hackers Execute Code Remotely	https://thehackernews.com/2025/10/severe-figma-mcp-vulnerability-lets.html
Critical Exploit Lets Hackers Bypass Authentication in WordPress Service Finder Theme	https://thehackernews.com/2025/10/critical-exploit-lets-hackers-bypass.html
CL0P-Linked Hackers Breach Dozens of Organizations Through Oracle Software Flaw	https://thehackernews.com/2025/10/cl0p-linked-hackers-breach-dozens-of.html
Gladinet CentreStack And Triofox 0-Day RCE Vulnerability Actively Exploited In Attacks	https://cybersecuritynews.com/gladinet-centrestack-and-triofox-0-day-rce/
7-Zip Vulnerabilities Let Attackers Execute Arbitrary Code Remotely	https://cybersecuritynews.com/7-zip-vulnerabilities/
Multiple Chrome Vulnerabilities Expose Users to Arbitrary Code Execution Attacks	https://cybersecuritynews.com/multiple-chrome-vulnerabilities/
Microsoft Azure Faces Global Outage Affecting Services Worldwide	https://cybersecuritynews.com/microsoft-azure-global-outage/
Linux Kernel ksmbd Filesystem Vulnerability Exploited – PoC Released	https://cybersecuritynews.com/linux-kernel-ksmbd-vulnerability-exploited/

CrowdStrike Falcon Windows Sensor Vulnerability Let Attacker Delete Arbitrary Files	https://cybersecuritynews.com/crowdstrike-falcon-windows-sensor-vulnerability/
FreePBX SQL Injection Vulnerability Exploited to Modify The Database	https://cybersecuritynews.com/freepbx-sql-injection-vulnerability/
Google's New AI Agent, CodeMender, Automatically Rewrites Vulnerable Code	https://cybersecuritynews.com/codemender-rewrites-vulnerable-code/
CISA Warns of Zimbra Collaboration Suite (ZCS) XSS Zero-Day Vulnerability Actively Exploited in Attacks	https://cybersecuritynews.com/cisa-zimbra-collaboration-suite-xss-zero-day/

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
GitLab Security Update – Patch For Multiple Vulnerabilities That Enables DoS Attack	https://cybersecuritynews.com/gitlab-security-update-vulnerabilities/
ClamAV 1.5.0 Released with New MS Office and PDF Verification Features	https://cybersecuritynews.com/clamav-1-5-0-released/

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
RondoDox botnet targets 56 n-day flaws in worldwide attacks	https://www.bleepingcomputer.com/news/security/rondodox-botnet-targets-56-n-day-flaws-in-worldwide-attacks/
SnakeKeylogger via Weaponized E-mails Leverage PowerShell to Exfiltrate Sensitive Data	https://cybersecuritynews.com/snakekeylogger-via-weaponized-e-mails/
New Polymorphic Python Malware Repeatedly Mutate its Appearance at Every Execution Time	https://cybersecuritynews.com/new-polymorphic-python-malware-repeatedly-mutate/
Attacks on Palo Alto PAN-OS Global Protect Login Portals Surge from 2,200 IPs	https://cybersecuritynews.com/attacks-on-palo-alto-global-protect-surge/
ASCII Smuggling Attack Lets Hackers Manipulate Gemini to Deliver Smuggled Data to Users	https://cybersecuritynews.com/ascii-smuggling-attack-gemini/
Critical AWS ClientVPN for macOS Vulnerability Let Attackers Escalate Privileges	https://cybersecuritynews.com/aws-clientvpn-for-macos-vulnerability/
Chaos Ransomware Upgrades With Aggressive New C++ Variant	https://www.darkreading.com/threat-intelligence/chaos-ransomware-upgrades-aggressive-new-variant
Framelink Figma MCP Server Opens Orgs to Agentic AI Compromise	https://www.darkreading.com/vulnerabilities-threats/figma-mcp-server-agentic-ai-compromise

TamperedChef Malware as PDF Editor Harvest Browser Credentials and Allows Backdoor Access	**https://cybersecuritynews.com/tamperedchef-malware-as-pdf-editor/**
Mustang Panda Using New DLL Side-Loading Technique to Deliver Malware	**https://cybersecuritynews.com/mustang-panda-using-new-dll-side-loading/**
New Phishing Kit Automates Generation of ClickFix Attack Bypassing Security Measures	**https://cybersecuritynews.com/new-phishing-kit-automates-generation-of-clickfix-attack/**
Hackers Use DFIR Tool 'Velociraptor' to Attack VMware ESXi and Windows Servers with Ransomware	**https://cybersecuritynews.com/dfir-tool-velociraptor-exploited/**

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/