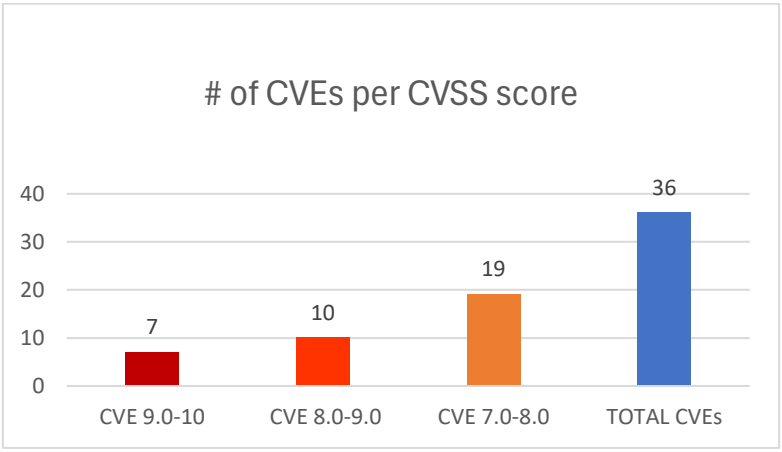
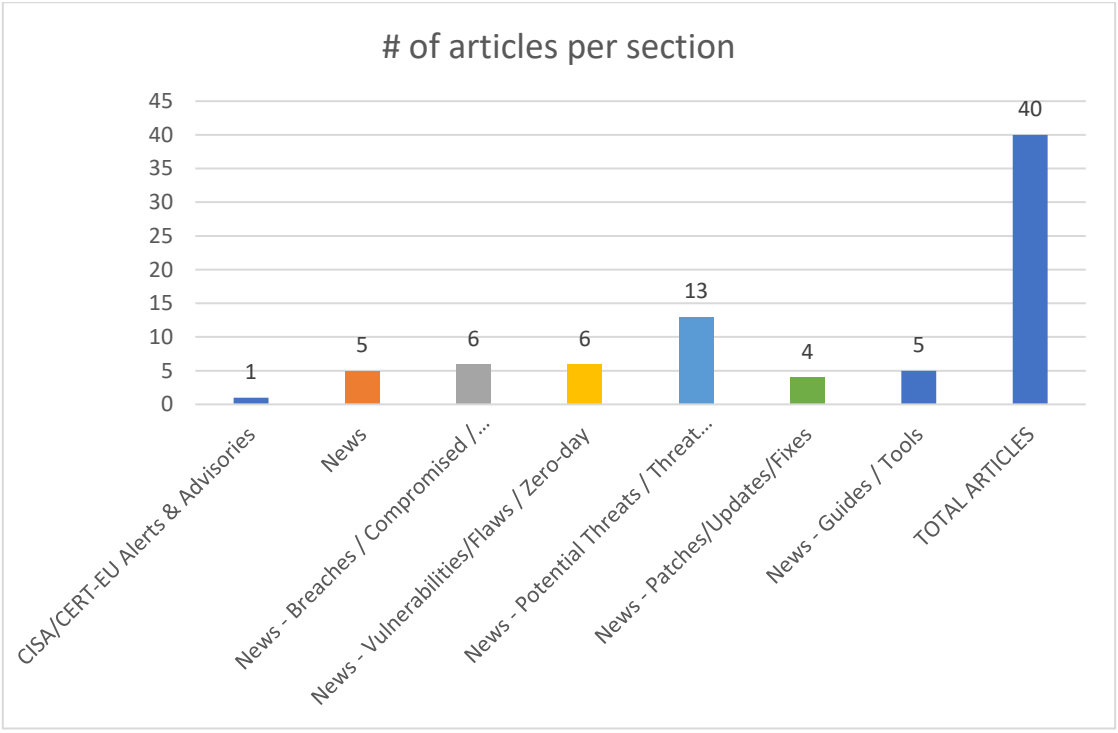
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 20/09/2025 - 23/09/2025





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-2025-59528	10,0	Flowise	Improper Control of Generation of Code ('Code Injection')	version 3.0.5	https://github.com/FlowiseAI/Flowise/blob/5930f1119c655bcf8d2200ae827a1f5b9fec81d0/packages/components/nodes/tools/MCP/CustomMCP/CustomMCP.ts#L132 GitHub, Inc. https://github.com/FlowiseAI/Flowise/blob/5930f1119c655bcf8d2200ae827a1f5b9fec81d0/packages/components/nodes/tools/MCP/CustomMCP/CustomMCP.ts#L220 GitHub, Inc. https://github.com/FlowiseAI/Flowise/blob/5930f1119c655bcf8d2200ae827a1f5b9fec81d0/packages/components/nodes/tools/MCP/CustomMCP/CustomMCP.ts#L262-L270 GitHub, Inc. https://github.com/FlowiseAI/Flowise/blob/5930f1119c655bcf8d2200ae827a1f5b9fec81d0/packages/server/src/controllers/nodes/index.ts#L57-L78 GitHub, Inc. https://github.com/FlowiseAI/Flowise/blob/5930f1119c655bcf8d2200ae827a1f5b9fec81d0/packages/server/src/routes/node-load-methods/index.ts#L5 GitHub, Inc. https://github.com/FlowiseAI/Flowise/blob/5930f1119c655bcf8d2200ae827a1f5b9fec81d0/packages/server/src/services/nodes/index.ts#L91-L94 GitHub, Inc. https://github.com/FlowiseAI/Flowise/releases/tag/flowise%403.0.6 GitHub, Inc. https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-3gcm-f6qx-ff7p

https://nvd.nist.gov/vuln/detail/CVE-2025-9321	9,8	The WPCasa plugin for WordPress	Improper Control of Generation of Code ('Code Injection')	all versions up to, and including, 1.4.1	https://plugins.trac.wordpress.org/browser/wpcasa/trunk/includes/class-wpsight-api.php#L48 Wordfence https://plugins.trac.wordpress.org/changeset/3365172/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/c1001b2b-395a-44ee-827e-6e57f7a50218?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-6544	9,8	h2oai/h2o-3	Deserialization of Untrusted Data	versions <= 3.46.0.8	https://github.com/h2oai/h2o-3/commit/0298ee348f5c73673b7b542158081e79605f5f25 huntr.dev https://huntr.com/bounties/53f35a0f-d644-4f82-93aa-89fe7e0aed40
https://nvd.nist.gov/vuln/detail/CVE-2025-35042	9,8	Airship AI Acropolis	Use of Default Credentials		https://raw.githubusercontent.com/cisagov/CSAF/develop/csaf_files/IT/white/2025/va-25-265-01.json Cybersecurity and Infrastructure Security Agency (CISA) U.S. Civilian Government https://www.cve.org/CVERecord?id=CVE-2025-35042
https://nvd.nist.gov/vuln/detail/CVE-2025-26399	9,8	SolarWinds Web Help Desk	Deserialization of Untrusted Data		https://documentation.solarwinds.com/en/success_center/whd/content/release_notes/whd_12-8-7-hotfix-1_release_notes.htm SolarWinds https://www.solarwinds.com/trust-center/security-advisories/CVE-2025-26399
https://nvd.nist.gov/vuln/detail/CVE-2025-56074	9,8	the foreigner-bwdates-reports-details.php file of PHPGurukul Park Ticketing Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	v2.0	https://github.com/baixiaobi/Park/blob/main/foreigner-bwdates-reports-details.php%20SQL%20Injection.md
https://nvd.nist.gov/vuln/detail/CVE-2025-57441	9,8	The Blackmagic ATEM Mini Pro	Exposure of Sensitive Information to an Unauthorized Actor	2.7	https://github.com/shiky8/my--cve-vulnerability-research/tree/main/CVE-2025-57441 MITRE https://www.blackmagicdesign.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-59572	8,8	WorkScout-Core	Cross-Site Request Forgery (CSRF)	from n/a through n/a	https://patchstack.com/database/wordpress/plugin/workscout-core/vulnerability/wordpress-workscout-core-plugin-1-7-06-cross-site-request-forgery-csrf-vulnerability?_s_id=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-10757	8,8	UTT 1200GW	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	up to 3.0.0-170831	https://github.com/cymiao1978/cve/blob/main/6.md VulDB https://github.com/cymiao1978/cve/blob/main/6.md#poc VulDB https://vuldb.com/?ctiid.325112 VulDB https://vuldb.com/?id.325112 VulDB https://vuldb.com/?submit.645681
https://nvd.nist.gov/vuln/detail/CVE-2025-10756	8,8	UTT HiPER 840G	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	up to 3.1.1-190328	https://github.com/cymiao1978/cve/blob/main/5.md VulDB https://github.com/cymiao1978/cve/blob/main/5.md#poc VulDB https://vuldb.com/?ctiid.325111 VulDB https://vuldb.com/?id.325111 VulDB https://vuldb.com/?submit.645678
https://nvd.nist.gov/vuln/detail/CVE-2025-10380	8,8	The Advanced Views – Display Posts, Custom Fields, and More plugin for WordPress	Improper Neutralization of Special Elements Used in a Template Engine	all versions up to, and including, 3.7.19	https://plugins.trac.wordpress.org/browser/acf-views/tags/3.7.19/src/Template_Engines/Twig.php#L106 Wordfence https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3364566%40acf-views&new=3364566%40acf-views&sfp_email=&sfph_mail= Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/52b04517-f0be-4bbf-818c-70a12d76bfec?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-10803	8,8	Tenda AC23	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	up to 16.03.07.52	https://github.com/lin-3-start/lin-cve/blob/main/Tenda%20AC23-3/Tenda%20AC23%20Buffer%20overflow.md VulDB https://vuldb.com/?ctiid.325161 VulDB https://vuldb.com/?id.325161 VulDB https://vuldb.com/?submit.654237 VulDB https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-10792	8,8	D-Link DIR-513	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	A1FW110	https://github.com/panda666-888/vuls/blob/main/d-link/dir-513/formWPS.md VulDB https://github.com/panda666-888/vuls/blob/main/d-link/dir-513/formWPS.md#poc VulDB https://vuldb.com/?ctiid.325149 VulDB https://vuldb.com/?id.325149 VulDB

					https://vuldb.com/?submit.654049 VulDB https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-43953	8,8	2wcom IP-4c	Improper Neutralization of Special Elements used in a Command ('Command Injection')	2.16	https://2wcom.com MITRE https://github.com/shiky8/my--cve-vulnerability-research/tree/main/CVE-2025-43953
https://nvd.nist.gov/vuln/detail/CVE-2025-57439	8,8	Creacast Creabox Manager	Improper Control of Generation of Code ('Code Injection')	4.4.4	http://www.creacast.com/ MITRE https://github.com/shiky8/my--cve-vulnerability-research/tree/main/CVE-2025-57439
https://nvd.nist.gov/vuln/detail/CVE-2025-57431	8,8	The Sound4 PULSE-ECO	Download of Code Without Integrity Check	AES67 1.22	https://github.com/shiky8/my--cve-vulnerability-research/tree/main/CVE-2025-57431 MITRE https://www.sound4.com
https://nvd.nist.gov/vuln/detail/CVE-2025-59430	8,2	Mesh Connect JS SDK	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Prior to version 3.3.2	https://github.com/FrontFin/mesh-web-sdk/blob/cf013b85ab95d64c63cbe46d6cb14695474924e7/packages/link/src/Link.ts#L441 GitHub, Inc. https://github.com/FrontFin/mesh-web-sdk/commit/7f22148516d58e21a8b7670dde927d614c0d15c2 GitHub, Inc. https://github.com/FrontFin/mesh-web-sdk/pull/124 GitHub, Inc. https://github.com/FrontFin/mesh-web-sdk/security/advisories/GHSA-vh3f-qppr-j97f
https://nvd.nist.gov/vuln/detail/CVE-2025-8892	7,8	Autodesk products	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')		https://www.autodesk.com/products/autodesk-access/overview Autodesk https://www.autodesk.com/trust/security-advisories/adsk-sa-2025-0019
https://nvd.nist.gov/vuln/detail/CVE-2025-5962	7,7	Lightspeed history service	Improper Access Control		https://access.redhat.com/errata/RHSA-2025:16345 Red Hat, Inc. https://access.redhat.com/errata/RHSA-2025:16346 Red Hat, Inc. https://access.redhat.com/security/cve/CVE-2025-5962 Red Hat, Inc. https://bugzilla.redhat.com/show_bug.cgi?id=2371363

https://nvd.nist.gov/vuln/detail/CVE-2025-59570	7,6	WPFunnels Mail Mint	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	from n/a through 1.18.6	https://patchstack.com/database/wordpress/plugin/mail-mint/vulnerability/wordpress-mail-mint-plugin-1-18-6-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-59588	7,5	PenciDesign Soledad	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusio	from n/a through 8.6.8	https://patchstack.com/database/wordpress/theme/soledad/vulnerability/wordpress-soledad-theme-8-6-8-local-file-inclusion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-59420	7,5	Authlib	Incorrect Authorization	Prior to version 1.6.4	https://github.com/authlib/authlib/commit/6b1813e4392eb7c168c276099ff7783b176479df GitHub, Inc. https://github.com/authlib/authlib/security/advisories/GHSA-9ggr-2464-2j32
https://nvd.nist.gov/vuln/detail/CVE-2025-58973	7,5	Easy Elementor Addons	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusio	from n/a through 2.2.8	https://patchstack.com/database/wordpress/plugin/easy-elementor-addons/vulnerability/wordpress-easy-elementor-addons-plugin-2-2-8-local-file-inclusion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-36202	7,5	IBM webMethods Integration	Use of Externally-Controlled Format String	10.15 and 11.1	https://www.ibm.com/support/pages/node/7245720
https://nvd.nist.gov/vuln/detail/CVE-2025-10813	7,3	Hostel Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ VulDB https://github.com/yihaofuweng/cve/issues/29 VulDB https://vuldb.com/?ctiid.325171 VulDB https://vuldb.com/?id.325171 VulDB https://vuldb.com/?submit.654438
https://nvd.nist.gov/vuln/detail/CVE-2025-10810	7,3	Campcodes Online Learning Management System	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	1.0	https://github.com/luyisi-7/CVE/issues/1 VulDB https://vuldb.com/?ctiid.325168 VulDB https://vuldb.com/?id.325168 VulDB https://vuldb.com/?submit.654435 VulDB https://www.campcodes.com/

https://nvd.nist.gov/vuln/detail/CVE-2025-10802	7,3	Online Bidding System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ VulDB https://github.com/peri0d/my_cve/blob/main/ONLINE-BIDDING-SYSTEM-Project-V1.0-remove.php-SQL-injection.md VulDB https://vuldb.com/?ctiid.325160 VulDB https://vuldb.com/?id.325160 VulDB https://vuldb.com/?submit.654164
https://nvd.nist.gov/vuln/detail/CVE-2025-10793	7,3	E-Commerce Website	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ VulDB https://github.com/K1nakoo/cve/blob/main/31/report.md VulDB https://vuldb.com/?ctiid.325150 VulDB https://vuldb.com/?id.325150 VulDB https://vuldb.com/?submit.654058
https://nvd.nist.gov/vuln/detail/CVE-2025-10801	7,3	Source-Codester Pet Grooming Management Software	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/YunyiLiu31/sql-injection-vulnerability VulDB https://vuldb.com/?ctiid.325158 VulDB https://vuldb.com/?id.325158 VulDB https://vuldb.com/?submit.654161 VulDB https://vuldb.com/?submit.655882 VulDB https://www.sourcecodester.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-10800	7,3	Online Discussion Forum	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/JunGu-W/cve/issues/14 VulDB https://github.com/JunGu-W/cve/issues/15 VulDB https://itsourcecode.com/ VulDB https://vuldb.com/?ctiid.325157 VulDB https://vuldb.com/?id.325157 VulDB https://vuldb.com/?submit.654152 VulDB https://vuldb.com/?submit.654153
https://nvd.nist.gov/vuln/detail/CVE-2025-55888	7,3	the Ajax transaction manager endpoint of ARD	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')		http://alpes.com MITRE http://ard.com MITRE https://github.com/0xZeroSec/CVE-2025-55888 MITRE https://services.ard.fr/?eID=tx_afereload_ajax_transactionmanager
https://nvd.nist.gov/vuln/detail/CVE-2025-53465	7,2	GSheets Connector	Deserialization of Untrusted Data	from n/a through 1.1.1	https://patchstack.com/database/wordpress/plugin/sheetlink/vulnerability/wordpress-gsheets-connector-plugin-1-1-1-php-object-injection-vulnerability?_s_id=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-59335	7,1	CubeCart	Insufficient Session Expiration	Prior to version 6.5.11	https://github.com/cubecart/v6/commit/4bfaeb4485dd82255a108940a163af5ba4583b52 GitHub, Inc. https://github.com/cubecart/v6/commit/62d9be8416aa6fd7343f8932d98c5b112b163e26 GitHub, Inc. https://github.com/cubecart/v6/security/advisories/GHSA-4vwh-x8m2-fmvv
https://nvd.nist.gov/vuln/detail/CVE-2025-58690	7,1	ptibogxiv Doliconnect	Cross-Site Request Forgery (CSRF)	from n/a through 9.5.7.	https://patchstack.com/database/wordpress/plugin/doliconnect/vulnerability/wordpress-doliconnect-plugin-9-5-7-cross-site-request-forgery-csrf-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-58688	7,1	Casengo Casengo Live Chat Support	Cross-Site Request Forgery (CSRF)	from n/a through 2.1.4	https://patchstack.com/database/wordpress/plugin/the-casengo-chat-widget/vulnerability/wordpress-casengo-live-chat-support-plugin-2-1-4-cross-site-request-forgery-csrf-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-53692	7,1	Sitecore Experience Platform (XP)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Sitecore Experience Manager (XM): from 9.2 through 10.4; Experience Platform (XP): from 9.2 through 10.4.	https://chudypb.github.io/ Wiz https://labs.watchtowr.com/disclosed-vulnerabilities/ Wiz https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1003734

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
SonicWall Releases Advisory for Customers after Security Incident		**https://www.cisa.gov/news-events/alerts/2025/09/22/sonicwall-releases-advisory-customers-after-security-incident**

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
Airport Chaos Shows Human Impact of 3rd-Party Attacks	**https://www.darkreading.com/cyberattacks-data-breaches/airport-chaos-human-impact-3rd-party-attacks**
Iran-Linked Hackers Target Europe With New Malware	https://www.darkreading.com/cyberattacks-data-breaches/iran-linked-hackers-europe-new-malware
Canada dismantles TradeOgre exchange, seizes $40 million in crypto	https://www.bleepingcomputer.com/news/security/canada-dismantles-tradeogre-exchange-seizes-40-million-in-crypto/
FBI Says Threat Actors Are Spoofing its IC3 Site	**https://www.infosecurity-magazine.com/news/fbi-says-threat-actors-are/**
Major Cyber Threat Detection Vendors Pull Out of MITRE Evaluations Test	**https://www.infosecurity-magazine.com/news/cyber-vendors-pull-out-mitre/**

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
Tiffany Data Breach Impacts Thousands of Customers	https://www.securityweek.com/tiffany-data-breach-impacts-thousands-of-customers/?&web_view=true
Ransomware gang says it hacked Spartanburg County, SC	https://www.comparitech.com/news/ransomware-gang-says-it-hacked-spartanburg-county-nc-employee-data/?&web_view=true
A Cyberattack on Jaguar Land Rover Is Causing a Supply Chain Disaster	https://www.wired.com/story/jlr-jaguar-land-rover-cyberattack-supply-chain-disaster/?&web_view=true
Day of delays at Heathrow after cyber-attack brings disruption	https://www.bbc.com/news/articles/c3drpgv33pxo?&web_view=true
22.2 Tbps DDoS Attack Breaks Internet With New World Record	https://cybersecuritynews.com/ddos-attack-world-record/
Stellantis, the Maker of Citroën, FIAT, Jeep, and Other Cars, Confirms Data Breach	https://cybersecuritynews.com/stellantis-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
American Archive of Public Broadcasting fixes bug exposing restricted media	https://www.bleepingcomputer.com/news/security/american-archive-of-public-broadcasting-fixes-bug-exposing-restricted-media/
Chrome Type Confusion 0-Day Vulnerability Code Analysis Released	https://cybersecuritynews.com/chrome-0-day-vulnerability-analysis/
SonicWall Urges Urgent Credential Reset After Backup File Exposure	https://www.esecurityplanet.com/news/sonicwall-urges-urgent-credential-reset-after-backup-file-exposure/?&web_view=true
Top Zero-Day Vulnerabilities Exploited in the Wild in 2025	https://cybersecuritynews.com/popular-zero-day-vulnerabilities/
First-ever AI-powered 'MalTerminal' Malware Uses OpenAI GPT-4 to Generate Ransomware Code	https://cybersecuritynews.com/first-ever-ai-powered-malterminal-malware/
Unpatched Fortra GoAnywhere instances at risk of full takeover (CVE-2025-10035)	https://www.helpnetsecurity.com/2025/09/22/fortra-goanywhere-vulnerability-cve-2025-10035/

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
Microsoft Patches Critical Entra ID Flaw Enabling Global Admin Impersonation Across Tenants	https://thehackernews.com/2025/09/microsoft-patches-critical-entra-id.html
Windows 11 24H2 Update KB5064081 Breaks Video Content Playback	https://cybersecuritynews.com/windows-11-24h2-update-video/
Microsoft lifts Windows 11 update block after face detection fix	https://www.bleepingcomputer.com/news/microsoft/microsoft-removes-windows-11-safeguard-hold-after-fixing-face-detection-bug/
Fortra Patches Critical GoAnywhere MFT Vulnerability	https://www.securityweek.com/fortra-patches-critical-goanywhere-mft-vulnerability/

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
BlockBlasters Steam Game Downloads Malware to Computer Disguised as Patch	https://cybersecuritynews.com/blockblasters-steam-game-downloads-malware/
Threat Actors Leverage Oracle Database Scheduler to Gain Access to Corporate Environments	https://cybersecuritynews.com/threat-actors-leverage-oracle-database-scheduler/
New Inboxfuscation Tool That Bypasses Microsoft Exchange Inbox Rules and Evade Detection	https://cybersecuritynews.com/inboxfuscation-tool/
ShadowLeak Exploit Exposed Gmail Data Through ChatGPT Agent	https://hackread.com/shadowleak-exploit-exposed-gmail-data-chatgpt-agent/
New EDR-Freeze Tool That Puts EDRs and Antivirus Into A Coma State	https://cybersecuritynews.com/edr-freeze-tool/
Threat Actors Selling New Undetectable RAT as 'ScreenConnect FUD Alternative'	https://cybersecuritynews.com/fud-as-screenconnect/
BlackLock Ransomware Attacking Windows, Linux, and VMware ESXi Environments	https://cybersecuritynews.com/blacklock-ransomware/
Subtle Snail Mimic as HR Representatives to Engage Employees and Steal Login Credentials	https://cybersecuritynews.com/subtle-snail-mimic-as-hr-representatives/

Kawa4096 Ransomware Attacking Multinational Organizations to Exfiltrate Sensitive Data	**https://cybersecuritynews.com/kawa4096-ransomware-attacking-multinational-organizations/**
New Botnet Leverages DNS Misconfiguration to Launch Massive Cyber Attack	**https://cybersecuritynews.com/new-botnet-leverages-dns-misconfiguration/**
Massive Cyber-Attack Attacking macOS Users via GitHub Pages to Deliver Stealer Malware	**https://cybersecuritynews.com/cyber-attack-attacking-macos-users/**
Hackers Bypassing Windows Mark of the Web Files Using LNK Stomping Attack	**https://cybersecuritynews.com/windows-mark-of-the-web-files-lnk-stomping/**
Lucid PhaaS With 17,500 Phishing Domains Mimics 316 Brands From 74 Countries	**https://cybersecuritynews.com/lucid-phaas-with-17500-phishing-domains/**

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/

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/