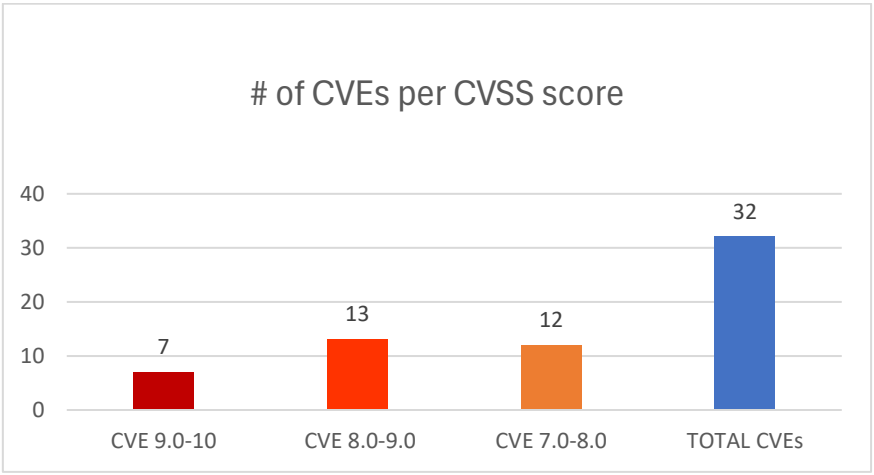
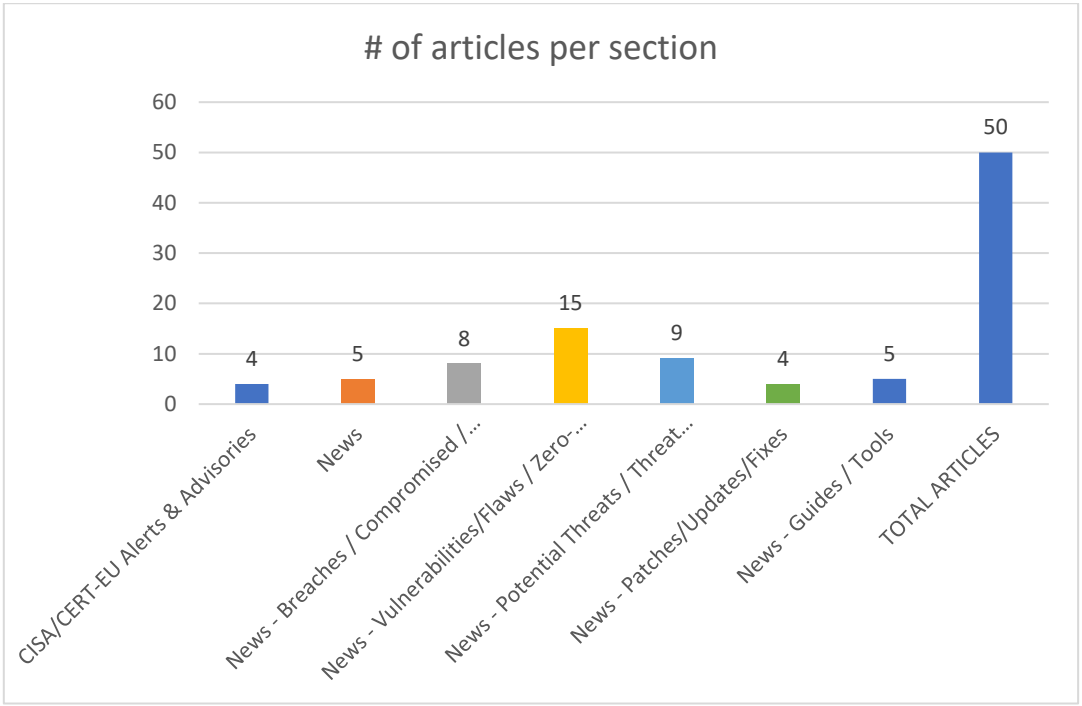
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 24/09/2025 - 26/09/2025





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-2025-9054	9,8	The MultiLoca - WooCommerce Multi Locations Inventory Management plugin for WordPress	Missing Authorization	all versions up to, and including, 4.2.8.	https://codecanyon.net/item/woocommerce-multi-locations-inventory-management/28949586#item-description__changelog Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/6a04e6ad-9365-4cb5-a0a0-82e047647d6b?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-21483	9,8	UE	Improper Restriction of Operations within the Bounds of a Memory Buffer		https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2025-bulletin.html
https://nvd.nist.gov/vuln/detail/CVE-2025-56819	9,8	Datart	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	v.1.0.0-rc.3	https://github.com/h2database/h2database MITRE https://github.com/xyyzxc/CVE-2025-56819 MITRE https://h2database.com/html/features.html#runscript
https://nvd.nist.gov/vuln/detail/CVE-2025-59834	9,8	ADB MCP Server is a MCP (Model Context Protocol) server for interacting with Android devices through AD	Improper Neutralization of Special Elements used in a Command ('Command Injection')	In versions 0.1.0 and prior	https://github.com/srmorete/adb-mcp/blob/master/src/index.ts#L334-L355 GitHub, Inc. https://github.com/srmorete/adb-mcp/commit/041729c0b25432df3199ff71b3163a307cf4c28c GitHub, Inc. https://github.com/srmorete/adb-mcp/security/advisories/GHSA-54j7-grvr-9xwg
https://nvd.nist.gov/vuln/d	9,6	the Nx (build system)	Embedded Malicious Code		https://access.redhat.com/security/cve/CVE-2025-10894 Red Hat, Inc. https://access.redhat.com/security/supply-chain-attacks-NPM-packages Red Hat, Inc. https://bugzilla.redhat.com/show_bug.cgi?id=2396282 Red Hat, Inc.

etail/CVE-2025-10894					https://github.com/nrwl/nx/security/advisories/GHSA-cxm3-wv7p-598c CISA-ADP, Inc., Red Hat https://www.stepsecurity.io/blog/supply-chain-security-alert-popular-nx-build-system-package-compromised-with-data-stealing-malware CISA-ADP, Inc., Red Hat https://www.wiz.io/blog/s1ngularity-supply-chain-attack
https://nvd.nist.gov/vuln/detail/CVE-2025-52906	9,3	TOTOLINK X6000R	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	through V9.4.0cu.1360_B20241207	https://github.com/PaloAltoNetworks/u42-vulnerability-disclosures/blob/main/2025/PANW-2025-0002/PANW-2025-0002.md Palo Alto Networks, Inc. https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/247/ids/36.html
https://nvd.nist.gov/vuln/detail/CVE-2025-10890	9,1	V8 in Google Chrome	Observable Discrepancy	prior to 140.0.7339.207	https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_23.html Chrome Release Notes Vendor Advisory https://issues.chromium.org/issues/430336833
https://nvd.nist.gov/vuln/detail/CVE-2025-10467	8,9	PROLIZ Computer Software Hardware Service Trade Ltd. Co. OBS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	before v25.0401	https://www.usom.gov.tr/bildirim/tr-25-0298
https://nvd.nist.gov/vuln/detail/CVE-2025-10500	8,8	Dawn in Google Chrome	Use After Free	prior to 140.0.7339.185	https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_17.html Chrome Release Notes Vendor Advisory https://issues.chromium.org/issues/435875050
https://nvd.nist.gov/vuln/detail/CVE-2025-10501	8,8	WebRTC in Google Chrome	Use After Free	prior to 140.0.7339.185	https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_17.html Chrome Release Notes Vendor Advisory https://issues.chromium.org/issues/440737137
https://nvd.nist.gov/vuln/detail/CVE-2025-10502	8,8	ANGLE in Google Chrome	Heap-based Buffer Overflow	prior to 140.0.7339.185	https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_17.html Chrome Release Notes Vendor Advisory https://issues.chromium.org/issues/438038775

https://nvd.nist.gov/vuln/detail/CVE-2025-10585	8,8	V8 in Google Chrome	Access of Resource Using Incompatible Type ('Type Confusion')	prior to 140.0.7339.185	https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_17.html Chrome Release Notes Vendor Advisory https://issues.chromium.org/issues/445380761
https://nvd.nist.gov/vuln/detail/CVE-2025-20334	8,8	HTTP API subsystem of Cisco IOS XE Software	Improper Neutralization of Special Elements used in a Command ('Command Injection')		https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cmd-inject-rPJM8BGL
https://nvd.nist.gov/vuln/detail/CVE-2025-10942	8,8	H3C Magic B3	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	up to 100R002	https://github.com/lin-3-start/lin-cve/blob/main/H3C%2BMagic%2BB3/H3C%20routers%20Buffer%20overflow.md VulDB https://github.com/lin-3-start/lin-cve/blob/main/H3C%2BMagic%2BB3/H3C%20routers%20Buffer%20overflow.md#poc VulDB https://vuldb.com/?ctiid.325812 VulDB https://vuldb.com/?id.325812 VulDB https://vuldb.com/?submit.651813
https://nvd.nist.gov/vuln/detail/CVE-2025-10948	8,8	MikroTik RouterOS 7	Improper Restriction of Operations within the Bounds of a Memory Buffer		https://github.com/a2ure123/libjson-unicode-buffer-overflow-poc CISA-ADP, VulDB https://github.com/a2ure123/libjson-unicode-buffer-overflow-poc#technical-proof-of-concept VulDB https://vuldb.com/?ctiid.325818 VulDB https://vuldb.com/?id.325818 VulDB https://vuldb.com/?submit.652387
https://nvd.nist.gov/vuln/detail/CVE-2025-59839	8,6	The EmbedVideo Extension is a MediaWiki	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	In versions 4.0.0 and prior	https://github.com/StarCitizenWiki/mediawiki-extensions-EmbedVideo/blob/440fb331a84b2050f4cc084c1d31d58a1d1c202d/resources/ext.embedVideo.videolink.js#L5-L20 GitHub, Inc. https://github.com/StarCitizenWiki/mediawiki-extensions-EmbedVideo/blob/440fb331a84b2050f4cc084c1d31d58a1d1c202d/resources/modules/iframe.js#L139-L155 GitHub, Inc. https://github.com/StarCitizenWiki/mediawiki-extensions-EmbedVideo/commit/4e075d3dc9a15a3ee53f449a684d5ab847e52f01 GitHub, Inc. https://github.com/StarCitizenWiki/mediawiki-extensions-EmbedVideo/security/advisories/GHSA-4j5h-mvj3-m48v

https://nvd.nist.gov/vuln/detail/CVE-2025-10438	8,6	Yordam Information Technology Consulting Education and Electrical Systems Industry Trade Inc. Yordam Katalog	Path Traversal: 'dir/../../filename'	before 21.7	https://www.usom.gov.tr/bildirim/tr-25-0296
https://nvd.nist.gov/vuln/detail/CVE-2025-10449	8,6	Saysis Computer Systems Trade Ltd. Co. Saysis Web Portal	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	from 3.1.9 & 3.2.0 before 3.2.1	https://www.usom.gov.tr/bildirim/tr-25-0297
https://nvd.nist.gov/vuln/detail/CVE-2025-10906	8,4	Magnetism Studios Endurance	Improper Authentication	up to 3.3.0 on macOS	https://github.com/SwayZGl1tZyyy/n-days/blob/main/Endurance/README.md VulDB https://github.com/SwayZGl1tZyyy/n-days/blob/main/Endurance/README.md#proof-of-concept VulDB https://vuldb.com/?ctiid.325691 VulDB https://vuldb.com/?id.325691 VulDB https://vuldb.com/?submit.653994
https://nvd.nist.gov/vuln/detail/CVE-2025-20160	8,1	TACACS+ protocol in Cisco IOS Software and Cisco IOS XE Software	Improper Authentication		https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-tacacs-hdB7thJw
https://nvd.nist.gov/vuln/detail/CVE-2025-58317	7,8	Delta Electronics CNCSoft-G2	Stack-based Buffer Overflow		https://filecenter.deltaww.com/news/download/doc/Delta-PCSA-2025-00017_CNCSoft-G2_File%20Parsing%20Stack-based%20Buffer%20Overflow%20Vulnerability.pdf
https://nvd.nist.gov/vuln/detail/CVE-2025-23348	7,8	NVIDIA Megatron-LM	Improper Control of Generation of Code ('Code Injection')		https://nvd.nist.gov/vuln/detail/CVE-2025-23348 NVIDIA Corporation https://nvidia.custhelp.com/app/answers/detail/a_id/5698 NVIDIA Corporation https://www.cve.org/CVERecord?id=CVE-2025-23348
https://nvd.nist.gov/vuln/detail/CVE-2025-27032	7,8	PIL authenticated VM	Improper Access Control Applied to Mirrored or Aliased Memory Regions		https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2025-bulletin.html

https://nvd.nist.gov/vuln/detail/CVE-2025-20352	7,7	Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software	Stack-based Buffer Overflow		https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte
https://nvd.nist.gov/vuln/detail/CVE-2025-59826	7,6	Flag Forge is a Capture The Flag (CTF) platform	Missing Authorizatio	version 2.1.0	https://github.com/FlagForgeCTF/flagForge/security/advisories/GHSA-q7pg-qchv-3pc5
https://nvd.nist.gov/vuln/detail/CVE-2025-55038	7,6	Click Plus C2-03CPU2	Missing Authorization	version 3.60	https://www.automationdirect.com/support/software-downloads ICS-CERT https://www.cisa.gov/news-events/ics-advisories/icsa-25-266-01
https://nvd.nist.gov/vuln/detail/CVE-2025-59305	7,6	Langfuse	Improper Authorization	3.1 before d67b317	https://depthfirst.com/post/how-an-authorization-flaw-reveals-a-common-security-blind-spot-cve-2025-59305-case-study
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-2025-57323	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-2025-55322	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-2025-48868	7,2	Horilla	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	1.3.0	https://drive.google.com/file/d/1XQAJilt77QxkjGEa94CsZRqZIZXa3ET9/view?usp=sharing GitHub, Inc. https://drive.google.com/file/d/1hnI9AK3fnpVrTlTRF7aRJsKhZCDIm2Ve/view?usp=sharing GitHub, Inc. https://github.com/horilla-opensource/horilla/commit/b0aab62b3a5fe6b7114b5c58db129b3744b4d8cc GitHub, Inc. https://github.com/horilla-opensource/horilla/security/advisories/GHSA-h6qj-pwmx-wjhw
https://nvd.nist.gov/vuln/detail/CVE-2025-21482	7,1	RSA PKCS	Cryptographic Issues		https://docs.qualcomm.com/product/publicresources/securitybulletin/september-2025-bulletin.html

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 Directs Federal Agencies to Identify and Mitigate Potential Compromise of Cisco Devices	**CVE-2025-20333 and CVE-2025-20362**	**https://www.cisa.gov/news-events/alerts/2025/09/25/cisa-directs-federal-agencies-identify-and-mitigate-potential-compromise-cisco-devices**
CISA Releases One Industrial Control Systems Advisory	▪ **ICSA-25-268-01 Dingtian DT-R002**	**https://www.cisa.gov/news-events/alerts/2025/09/25/cisa-releases-one-industrial-control-systems-advisory**
ED 25-03: Identify and Mitigate Potential Compromise of Cisco Devices	▪ **CVE-2025-20333 – allows for remote code execution** ▪ **CVE-2025-20362 – allows for privilege escalation**	**https://www.cisa.gov/news-events/directives/ed-25-03-identify-and-mitigate-potential-compromise-cisco-devices**
Supplemental Direction ED 25-03: Core Dump and Hunt Instructions		**https://www.cisa.gov/news-events/directives/supplemental-direction-ed-25-03-core-dump-and-hunt-instructions**

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
Cisco's Wave of Actively Exploited Zero-Day Bugs Targets Firewalls, IOS	**https://www.darkreading.com/vulnerabilities-threats/cisco-actively-exploited-zero-day-bugs-firewalls-ios**
Experts Warn of Global Breach Risk from Indian Suppliers	https://www.infosecurity-magazine.com/news/experts-global-breach-risk-indian/
NCA Arrest Man as HardBit Ransomware Blamed for Airport Outages	https://www.infosecurity-magazine.com/news/nca-arrest-hardbit-ransomware/
New Domain-fronting Attack Uses Google Meet, YouTube, Chrome and GCP to Tunnel Traffic	**https://cybersecuritynews.com/domain-fronting-attack/**
New Russian Disinformation Campaign Targeting Upcoming Moldova's Elections	**https://cybersecuritynews.com/new-russian-disinformation-campaign/**

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
Malicious AI Agent Server Reportedly Steals Emails	https://www.infosecurity-magazine.com/news/malicious-ai-agent-server/
Vegas Gambling Giant Hit by Cyber Incident, Employee Data Exposed	https://www.infosecurity-magazine.com/news/vegas-gambling-cyber-incident/
Arizona school district notifies 35,000 of data breach following ransomware attack	https://www.comparitech.com/news/arizona-school-district-notifies-35000-of-data-breach-following-ransomware-attack/?&web_view=true
Boyd Gaming discloses data breach after suffering a cyberattack	https://www.bleepingcomputer.com/news/security/boyd-gaming-discloses-data-breach-after-suffering-a-cyberattack/?&web_view=true
Ransomware gang says it hacked the Maryland Department of Transportation	https://www.comparitech.com/news/ransomware-gang-says-it-hacked-the-maryland-transportation-department/?&web_view=true
Numerous Applications Using Google's Firebase Platform Leaking Highly Sensitive Data	https://cybersecuritynews.com/numerous-applications-using-googles-firebase-platform/
CISA Warns of Shai-Hulud Self-Replicating Worm Compromised 500+ Packages in npm Registry	https://cybersecuritynews.com/cisa-shai-hulud-npm-attack/
ShadowV2 Botnet Exploits Docker Containers on AWS to Turn Thems as Infected System for DDoS Attack	https://cybersecuritynews.com/shadowv2-botnet-exploits-docker-containers-on-aws/

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
Cisco ASA Firewall Zero-Day Exploits Deploy RayInitiator and LINE VIPER Malware	https://thehackernews.com/2025/09/cisco-asa-firewall-zero-day-exploits.html
State-Sponsored Hackers Exploiting Libraesva Email Security Gateway Vulnerability	https://thehackernews.com/2025/09/state-sponsored-hackers-exploiting.html
Hackers Exploit Pandoc CVE-2025-51591 to Target AWS IMDS and Steal EC2 IAM Credentials	https://thehackernews.com/2025/09/hackers-exploit-pandoc-cve-2025-51591.html

Two Critical Flaws Uncovered in Wondershare RepairIt Exposing User Data and AI Models	https://thehackernews.com/2025/09/two-critical-flaws-uncovered-in.html
Cisco Warns of Actively Exploited SNMP Vulnerability Allowing RCE or DoS in IOS Software	https://thehackernews.com/2025/09/cisco-warns-of-actively-exploited-snmp.html
Unpatched flaw in OnePlus phones lets rogue apps text messages	https://www.bleepingcomputer.com/news/security/unpatched-flaw-in-oneplus-phones-lets-rogue-apps-text-messages/
New Supermicro BMC flaws can create persistent backdoors	https://www.bleepingcomputer.com/news/security/new-supermicro-bmc-flaws-can-create-persistent-backdoors/
GeoServer Flaw Exploited in US Federal Agency Hack	https://www.securityweek.com/geoserver-flaw-exploited-in-us-federal-agency-hack/
ZendTo Vulnerability Let Attackers Bypass Security Controls and Access Sensitive Data	https://cybersecuritynews.com/zendto-vulnerability/
New LockBit 5.0 Ransomware Variant Attacking Windows, Linux, and ESXi Systems	https://cybersecuritynews.com/new-lockbit-5-0-ransomware-variant/
SetupHijack Tool Exploits Race Conditions and Insecure File Handling in Windows Installer Processes	https://cybersecuritynews.com/setuphijack-tool/
Linux Kernel ksmbd Vulnerability Allows Remote Attackers to Execute Arbitrary Code	https://cybersecuritynews.com/linux-kernel-ksmbd-vulnerability/
Critical DNN Platform Vulnerability Let Attackers Execute Malicious Scripts	https://cybersecuritynews.com/critical-dnn-platform-vulnerability/
Hackers Exploiting Hikvision Camera Vulnerability to Access Sensitive Information	https://cybersecuritynews.com/hikvision-camera-vulnerability/
CISA Warns of Google Chrome 0-Day Vulnerability Exploited in Attacks	https://cybersecuritynews.com/cisa-google-chrome-0-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
Salesforce Patches Critical ForcedLeak Bug Exposing CRM Data via AI Prompt Injection	https://thehackernews.com/2025/09/salesforce-patches-critical-forcedleak.html
Cisco Patches Zero-Day Flaw Affecting Routers and Switches	https://www.securityweek.com/cisco-patches-zero-day-flaw-affecting-routers-and-switches/
ShadowV2 Botnet Exposes Rise of DDoS-as-a-service Platforms	https://www.infosecurity-magazine.com/news/shadowv-botnet-ddos-service/
Kali Linux 2025.3 Released With New Features and 10 New Hacking Tools	https://cybersecuritynews.com/kali-linux-2025-3-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
Chinese Hackers RedNovember Target Global Governments Using Pantegana and Cobalt Strike	https://thehackernews.com/2025/09/chinese-hackers-rednovember-target.html
Chinese Hackers Use 'BRICKSTORM' Backdoor to Breach US Firms	https://www.infosecurity-magazine.com/news/chinese-hackers-brickstorm/
npm Package Uses QR Code Steganography to Steal Credentials	https://www.infosecurity-magazine.com/news/npm-uses-qr-code-steganography/
New Phishing Attack Targeting PyPI Maintainers to Steal Login Credentials	https://cybersecuritynews.com/new-phishing-attack-targeting-pypi-maintainers/
Hackers Exploiting WordPress Websites With Silent Malware to Gain Admin Access	https://cybersecuritynews.com/hackers-exploiting-wordpress-websites/
COLDRIVER APT Group Uses ClickFix To Deliver a New PowerShell-Based Backdoor BAITSWITCH	https://cybersecuritynews.com/coldriver-apt-group-uses-clickfix/
Banking Trojans Attacking Android Users Mimic as Government and Legitimate Payment Apps	https://cybersecuritynews.com/banking-trojans-attacking-android-users/
Hackers Exploit WerFaultSecure.exe Tool to Steal Cached Passwords From LSASS on Windows 11 24H2	https://cybersecuritynews.com/windows-11-cached-passwords/
Hackers Can Compromise Chromium Browsers in Windows by Loading Arbitrary Extensions	https://cybersecuritynews.com/chromium-browsers-windows-arbitrary-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
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/