

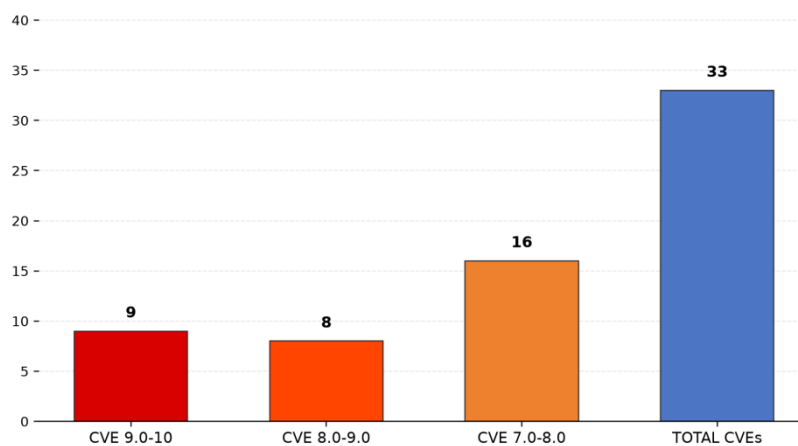


Newsletter on system vulnerabilities and cybersecurity news.

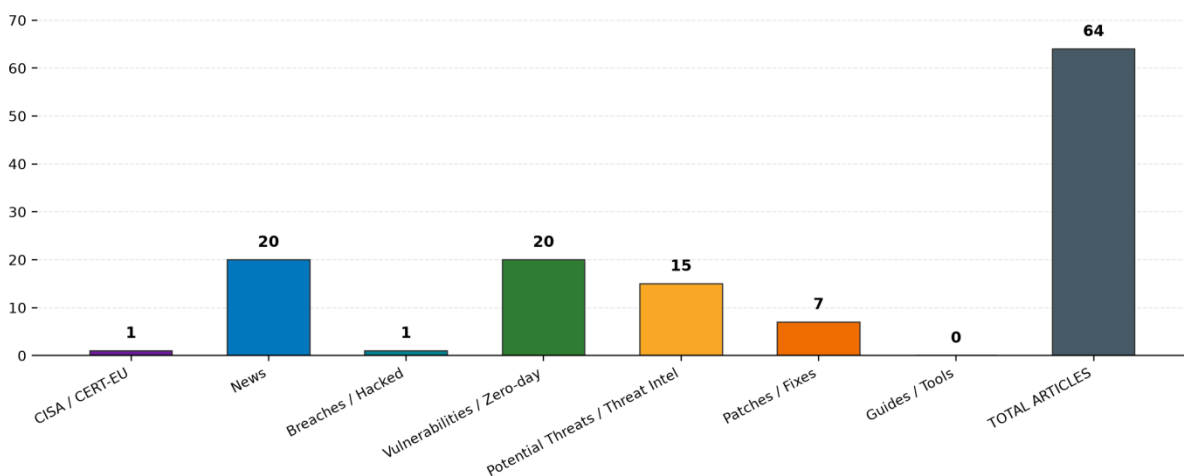
National Cyber Security Authority (NCSA)

Date: 30/09/2026 - 02/10/2026

of CVEs per CVSS score



of articles per section



Contents

Common Vulnerabilities and Exposures (CVEs)	3
CISA/CERT-EU Alerts & Advisories	7
News.....	7
Breaches / Compromised / Hacked.....	8
Vulnerabilities / Flaws / Zero-day.....	8
Patches / Updates / Fixes	10
Potential threats / Threat intelligence	10
Guides / Tools.....	11
References.....	12
Annex – Websites with vendor specific vulnerabilities	13

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 όπως ευπάθειας (όπως SQL injection ή command injection) και σχετικοί σύνδεσμοι για περαιτέρω πληροφόρηση ή μέτρα αντιμετώπισης.

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-102427	10,0	Joomla CCK	Unrestricted Upload of File with Dangerous Type	< 8.3	https://www.ordasoft.com/	none	yes	total
CVE-2026-103764	9,8	Mooncake transfer engine	Untrusted Pointer Dereference	before 0.3.13	https://github.com/kvccache-ai/Mooncake/blob/6041a609a8c3af35e778f70db344f145c2914980/mooncake-transfer-engine/src/transport/tcp_transport/tcp_transport.cpp#L209 https://github.com/kvccache-ai/Mooncake/commit/a2933849417259e562fc9cbad63c618d464dfb2d https://github.com/kvccache-ai/Mooncake/issues/4441 https://github.com/kvccache-ai/Mooncake/releases/tag/v0.3.13 https://www.vulncheck.com/advisories/mooncake-transfer-engine-before-0.3.13-unauthenticated-arbitrary-memory-read-write-via-tcp-transport			
CVE-2026-14378	9,8	The DevKit Pro plugin for WordPress	Improper Authentication	up to, and including, 2.3.0	https://docs.dplugins.com/devkit/changelog https://www.wordfence.com/threat-intel/vulnerabilities/id/2ab3986a-69e0-442f-8e79-35b1bc5376d9?source=cve			
CVE-2026-19660	9,8	The Divi Membership plugin for WordPress	Improper Authentication	up to, and including, 2.3.0.	https://diviengine.com/divi-membership-changelog/ https://www.wordfence.com/threat-intel/vulnerabilities/id/3d650cda-341f-4772-9b67-1bac200e3fb7?source=cve			
CVE-2026-76504	9,8	the API session-based authentication management of Cisco Catalyst SD-WAN Manager	Improper Handling of URL Encoding (Hex Encoding)	versions up to (excluding) 20.9.10.1; versions from (including) 20.12 up to (excluding) 20.12.8.2; versions from (including) 20.15 up to (excluding) 20.15.6.1; versions from (including) 20.18 up to (excluding) 20.18.4.1; versions from (including) 26.1 up to (excluding) 26.1.2.1; 26.2	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-webauth-xr8beuuU	active	yes	total
CVE-2026-103765	9,4	Mooncake	Missing Authentication for Critical Function	through 0.3.13.post1	https://github.com/kvccache-ai/Mooncake/blob/719735896c86b56fabec6cf3e825fb2ea640597a/mooncake-wheel/mooncake/http_metadata_server.py#L61-L106 https://github.com/kvccache-ai/Mooncake/issues/4444 https://www.vulncheck.com/advisories/mooncake-through-0.3.13-post1-missing-authentication-in-http-metadata-server			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-103922	9,3	Capacitor	Origin Validation Error; Unintended Proxy or Intermediary ('Confused Deputy')	>= 6.0.0, < 6.2.2; >= 7.0.0, < 7.6.9; >= 8.0.0, < 8.3.5; >= 8.3.5, < 8.4.3; >= 8.5.0, < 8.5.1	https://github.com/ionic-team/capacitor/commit/430356a91e1419fc66862dc09835081aa501677e https://github.com/ionic-team/capacitor/commit/80b6c5e81d062e1e158914040f49e044d95b7ccb https://github.com/ionic-team/capacitor/commit/85ccc44151fdd5ae5e0d806d875766ef4b84ad5d https://github.com/ionic-team/capacitor/commit/af9a287fef45f0ac68ce640cb42fed2d06b0f1b4 https://github.com/ionic-team/capacitor/commit/d5e3170ba0ff155fc542b7e6d16cff5201406540 https://github.com/ionic-team/capacitor/commit/ee586ae680887ba99d066616f976db149542d922	none	no	total
CVE-2026-55083	9,1	DHIS2	Deserialization of Untrusted Data	before 2.42.5.1; before 2.43.0.1	https://github.com/dhis2/dhis2-core/releases/tag/2.42.5.1 https://github.com/dhis2/dhis2-core/releases/tag/2.43.0.1 https://github.com/dhis2/dhis2-core/security/advisories/GHSA-3fr2-wvqx-cmr5	none	no	total
CVE-2026-86345	9,0	389-ds-base	Improper Restriction of Communication Channel to Intended Endpoints		https://access.redhat.com/security/cve/CVE-2026-86345 https://bugzilla.redhat.com/show_bug.cgi?id=2529332			
CVE-2026-102578	8,8	Moodle	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	versions up to (excluding) 4.5.13; versions from (including) 5.0.0 up to (excluding) 5.0.9; versions from (including) 5.1.0 up to (excluding) 5.1.6; versions from (including) 5.2.0 up to (excluding) 5.2.2	http://git.moodle.org/gw/?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-89383 https://access.redhat.com/security/cve/CVE-2026-102578 https://bugzilla.redhat.com/show_bug.cgi?id=2543632 https://moodle.org/mod/forum/discuss.php?d=482496	none	no	partial
CVE-2026-103484	8,8	pgvector	Out-of-bounds Write; Improper Validation of Specified Quantity in Input	before 0.8.7	https://github.com/pgvector/pgvector/commit/ee00d39ab30c2a7cf9510abf9288c624d91db156 https://github.com/pgvector/pgvector/issues/1036	none	no	total
CVE-2026-104018	8,8	the command shell of Wind River VxWorks 7	Improper Privilege Management	prior to 26.09.	https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2026-104018	none	no	total
CVE-2026-15897	8,8	The Super Forms – Drag & Drop Form Builder plugin for WordPress	Improper Privilege Management	up to, and including, 6.3.316.	https://github.com/RensTillmann/super-forms/pull/205 https://www.wordfence.com/threat-intel/vulnerabilities/id/94297481-9ebb-42cb-9362-be8bc52b126f?source=cve			
CVE-2026-54049	8,7	Sakai	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	before 23.5; before 25.3	https://github.com/sakaiproject/sakai/commit/2696b4b48cbef2e81512f52f84f7477adff78b27 https://github.com/sakaiproject/sakai/security/advisories/GHSA-w2x5-qv52-9ccv			
CVE-2026-104051	8,2	PictShare	Insufficiently Protected Credentials	before 3.7.1	https://github.com/HaschekSolutions/pictshare/commit/ce5fc474e89769efeae25fee763894bcce3412e3 https://github.com/HaschekSolutions/pictshare/releases/tag/v3.7.1 https://www.vulncheck.com/advisories/pictshare-sensitive-information-disclosure-via-info-api			
CVE-2026-103493	8,1	In JetBrains YouTrack	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	before 2026.2.19422	https://www.jetbrains.com/privacy-security/issues-fixed/	none	no	total

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-104059	8,1	Lektor	Cross-Site Request Forgery (CSRF)	3.3.14 and earlier; 3.4.0b1 through 3.4.0b15	https://gist.github.com/mansurmavlanlankulov/c7683e3204e84892e442b0196585d5bb https://www.vulncheck.com/advisories/lektor-csrf-via-admin-api-endpoints			
CVE-2023-54404	7,5	Zod schema-validation library	Allocation of Resources Without Limits or Throttling	through 4.6.5	https://github.com/colinhacks/zod/issues/1872 https://github.com/colinhacks/zod/pull/6475 https://www.vulncheck.com/advisories/zod-uncontrolled-resource-consumption-via-array-validation			
CVE-2024-58388	7,5	Sharp (and Toshiba Tec re-branded) multifunction printers	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')		https://github.com/projectdiscovery/nuclei-templates/blob/main/http/vulnerabilities/other/crocus-lfi.yaml https://pierrekim.github.io/blog/2024-06-27-sharp-mfp-17-vulnerabilities.html#pre-auth-lfi https://www.vulncheck.com/advisories/sharp-multifunction-printers-local-file-inclusion-via-installed-emanual-down.html			
CVE-2026-103096	7,5	GV-Eye	Cleartext Storage of Sensitive Information; Inclusion of Sensitive Information in Source Code; Use of Hard-coded Credentials	V3.6.0	https://www.geovision.com.tw/cyber_security.php			
CVE-2026-103098	7,5	the URL over an unencrypted HTTP connection	Cleartext Transmission of Sensitive Information	V3.6.0	https://www.geovision.com.tw/cyber_security.php			
CVE-2026-104020	7,5	the Ion reader in Amazon Ion Python	Uncontrolled Recursion	before 0.15.0; 0.15.0 or later	https://aws.amazon.com/security/security-bulletins/2026-122-aws/ https://github.com/amazon-ion/ion-python/releases/tag/v0.15.0 https://github.com/amazon-ion/ion-python/security/advisories/GHSA-93q6-f8hx-vv7f			
CVE-2026-104057	7,5	Podgrab	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	032248091294dbf5b6a439a5afd93788a7cc647f and earlier	https://gist.github.com/mansurmavlanlankulov/022bc672583687ccb34dcf4cb31b6188 https://www.vulncheck.com/advisories/podgrab-unauthenticated-dos-via-concurrent-map-access-in-websocket-handler	none	yes	partial
CVE-2026-68495	7,5	FasterXML jackson-dataformats-binary never invokes StreamReadConstraints	Uncontrolled Resource Consumption; Allocation of Resources Without Limits or Throttling	before 2.16.0	https://github.com/FasterXML/jackson-dataformats-binary/blob/2.18/release-notes/VERSION-2.x https://github.com/FasterXML/jackson-dataformats-binary/issues/725 https://github.com/FasterXML/jackson-dataformats-binary/security/advisories/GHSA-3v8f-v6vx-fmrm https://www.cve.org/CVERecord?id=CVE-2026-68496	poc	yes	partial
CVE-2026-103921	7,4	GraphQL Tools	Improper Certificate Validation	Prior to 1.1.35	https://github.com/ardatan/graphql-tools/commit/3831a0661514c91d99971052f983552556880402 https://github.com/ardatan/graphql-tools/pull/8426 https://github.com/ardatan/graphql-tools/releases/tag/@graphql-tools/executor-legacy-ws@1.1.35 https://github.com/ardatan/graphql-tools/security/advisories/GHSA-6fw5-9hg8-w87g	none	no	total
CVE-2026-104120	7,3	modelcontextprotocol mcp-server-fetch and mcp-server-everything	Server-Side Request Forgery (SSRF)	up to 2026.6.4.	https://github.com/modelcontextprotocol/servers/issues/4492 https://github.com/modelcontextprotocol/servers/pull/4890 https://vuldb.com/cve/CVE-2026-104120 https://vuldb.com/submit/960099 https://vuldb.com/vuln/412764 https://vuldb.com/vuln/412764/ctj			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-104123	7,3	SourceCoder Online Reviewer Management System	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'); Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/lemssh77/cve/issues/1 https://vuldb.com/cve/CVE-2026-104123 https://vuldb.com/submit/961692 https://vuldb.com/vuln/412765 https://vuldb.com/vuln/412765/cti https://www.sourcecodester.com/			
CVE-2026-101888	7,2	The Prime Mover plugin for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	before 2.2.1	https://wordpress.org/plugins/prime-mover/#developers https://www.vulncheck.com/advisories/prime-mover-zip-slip-path-traversal-file-write	none	no	total
CVE-2026-102565	7,2	The BA Book Everything plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 1.8.28	https://plugins.trac.wordpress.org/browser/ba-book-everything/tags/1.8.28/includes/class-babe-html.php#L3609 https://plugins.trac.wordpress.org/browser/ba-book-everything/tags/1.8.28/includes/class-babe-order.php#L1265 https://plugins.trac.wordpress.org/browser/ba-book-everything/tags/1.8.28/includes/class-babe-order.php#L2041 https://plugins.trac.wordpress.org/browser/ba-book-everything/tags/1.8.28/includes/class-babe-order.php#L2073 https://plugins.trac.wordpress.org/browser/ba-book-everything/tags/1.8.28/includes/class-babe-order.php#L2195 https://plugins.trac.wordpress.org/changeset?reponame=&new=3720938%40ba-book-everything&old=3709590%40ba-book-everything			
CVE-2026-103766	7,2	ClipBucket	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	v5 through 5.5.3-	https://github.com/MacWarrior/clipbucket-v5 https://github.com/MacWarrior/clipbucket-v5/blob/f15cef1a2431786c31fd79e81f55d6eeca4ebc0/upload/includes/classes/ads.class.php#L102-L110 https://github.com/MacWarrior/clipbucket-v5/pull/925 https://hackmd.io/@leediav/sql-i-via-delete-ads-clipbucketv5 https://www.vulncheck.com/advisories/clipbucket-v5-through-5.5.3-197-sql-injection-via-ads-manager-php-delete-parameter			
CVE-2026-53964	7,2	Document Merge Service	Improper Neutralization of Special Elements Used in a Template Engine	Prior to version 9.1.0	https://github.com/adfinis/document-merge-service/releases/tag/v9.1.0 https://github.com/adfinis/document-merge-service/security/advisories/GHSA-w47q-945m-g9pc	none	no	total
CVE-2026-90438	7,2	The Ninja Forms – The Contact Form Builder That Grows With You plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 3.15.4	https://plugins.trac.wordpress.org/browser/ninja-forms/tags/3.15.2/build/submissions.js#L1 https://plugins.trac.wordpress.org/browser/ninja-forms/tags/3.15.2/includes/AJAX/Controllers/Submitson.php#L61 https://plugins.trac.wordpress.org/browser/ninja-forms/tags/3.15.2/includes/Database/Models/Submitson.php#L308 https://plugins.trac.wordpress.org/browser/ninja-forms/tags/3.15.2/includes/Helper.php#L261 https://plugins.trac.wordpress.org/browser/ninja-forms/tags/3.15.3/build/submissions.js#L1 https://plugins.trac.wordpress.org/browser/ninja-forms/tags/3.15.3/includes/AJAX/Controllers/Submitson.php#L61			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-93367	7,2	The Visitors Traffic Real Time Statistics Pro plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 11.22	https://www.wordfence.com/threat-intel/vulnerabilities/id/a72261e5-7376-4a34-9264-27bd4f27e938?source=cve https://www.wp-buy.com/product/visitors-traffic-real-time-statistics-pro/			

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 CISA	CVE-2026-104286 Fortinet FortiMail Path Traversal Vulnerability	https://cisa.gov/news-events/alerts/2026/10/01/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
Treasury Sanctions Tren de Aragua ATM Jackpotting Network Linked to \$40.7 Million in Losses	https://cybersecuritynews.com/tren-de-aragua-atm-jackpotting
U.S. Arrests Tech Company Owner for Allegedly Smuggling \$300 Million in GPU Servers to China	https://cybersecuritynews.com/u-s-arrests-tech-company-owner
Autonomous AI agents tried to hack US, Canadian government websites	https://bleepingcomputer.com/news/security/autonomous-ai-agents-tried-to-hack-us-canadian-government-websites
Zero Trust Creator Says Model Holds Firm Against AI-Assisted Attacks	https://securityweek.com/zero-trust-creator-says-model-holds-firm-against-ai-assisted-attacks
Osavul Lands \$10 Million to Spot Hostile Intent Across Cyber, Physical Domains	https://securityweek.com/osavul-lands-10-million-to-spot-hostile-intent-across-cyber-physical-domains
FTC Investigating OpenAI, Anthropic and Other AI Models Over Potential Risks to Customers	https://cybersecuritynews.com/ftc-investigating-ai-models
16-year-old Alleged KillSec Ransomware Group Leader Arrested, Servers Dismantled	https://cybersecuritynews.com/16-year-old-leader-killsec-ransomware
Chinese Hackers Posing as Senior Anthropic Employee Targeting US AI Policy Experts	https://cybersecuritynews.com/chinese-hackers-posing-as-anthropic-employee
Hacker Conversations: Rob Juncker, a Knock at the Door and a Moral Compass	https://securityweek.com/hacker-conversations-rob-juncker-a-knock-at-the-door-and-a-moral-compass

Enterprises Struggle to Prepare for AI and Quantum Threats, PwC Says	https://securityweek.com/enterprises-struggle-to-prepare-for-ai-and-quantum-threats-pwc-says
China-Linked Hackers Impersonate AI Experts to Target US Policy	https://infosecurity-magazine.com/news/ta419-impersonates-ai-experts-us
AI Has Changed Attack Speed, Not Security Fundamentals	https://securityweek.com/ai-has-changed-attack-speed-not-security-fundamentals
How Financial Services Companies Can Modernize Their Software Supply Chain	https://thehackernews.com/2026/10/how-financial-services-companies-can.html
Kevin Mandia's Armadin Raises \$255 Million at \$2.5 Billion Valuation	https://securityweek.com/kevin-mandias-armadin-raises-255-million-at-2-5-billion-valuation
Microsoft enables Windows settings backup by default for orgs	https://bleepingcomputer.com/news/microsoft/microsoft-enables-windows-settings-backup-by-default-for-orgs
Zammad Zero-Days Exploited in AI-Powered DIVD Hack	https://securityweek.com/zammad-zero-days-exploited-in-ai-powered-divd-hack
OpenAI Disrupts Reasoning Extraction Campaign Linked to Moonshot AI Associates	https://thehackernews.com/2026/10/openai-disrupts-reasoning-extraction.html
CISA Adds Exploited Cisco Catalyst SD-WAN Manager Auth Bypass to KEV	https://thehackernews.com/2026/10/cisa-adds-exploited-cisco-catalyst-sd.html
AI Threats Top Cybersecurity Preparedness Gap, PwC Finds	https://infosecurity-magazine.com/news/mitigating-adversarial-ai-top
Google Rolls Out Gemini 4 Argon to Trusted Cyber Defenders, Plans Guardrail-Free Version	https://thehackernews.com/2026/10/google-rolls-out-gemini-4-argon-to.html

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
Hackers stole Pentagon personnel records of over 3 million people	https://bleepingcomputer.com/news/security/hackers-breach-pentagon-human-resources-management-system-steal-data-of-nearly-3-million-people

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
Exploited Fortinet FortiMail Zero-Day Calls for Urgent Action	https://securityweek.com/exploited-fortinet-fortimail-zero-day-calls-for-urgent-action
Critical FortiMail Zero-Day Flaw Exploited in Attacks Allows Unauthenticated Arbitrary File Writes	https://thehackernews.com/2026/10/critical-fortimail-zero-day-flaw.html
Multiple Apache HTTP Server Vulnerabilities Could Enable Code Execution Attacks	https://cybersecuritynews.com/apache-http-server-vulnerabilities-2

Critical Fortinet FortiMail 0-Day Vulnerability Actively Exploited in Attacks	https://cybersecuritynews.com/fortimail-0-day-vulnerability-exploited
Fortinet warns of critical FortiMail flaw exploited in zero-day attacks	https://bleepingcomputer.com/news/security/fortinet-warns-of-critical-fortimail-flaw-exploited-in-zero-day-attacks
ThreatsDay: AI-Powered Zero-Day Chain, 543K Live Secrets, Model Inspection RCE and 13 More Stories	https://thehackernews.com/2026/10/threatsday-ai-powered-zero-day-chain.html
Critical Cisco Catalyst SD-WAN Zero-Day Under Active Exploitation	https://infosecurity-magazine.com/news/critical-cisco-catalyst-sdwan
Node.js ImageResponse Implementation Vulnerability Enables Remote Code Execution	https://cybersecuritynews.com/node-js-imageresponse-implementation-vulnerability
Zimbra Vulnerability Exploited in the Wild Prior to Public Disclosure	https://securityweek.com/zimbra-vulnerability-exploited-in-the-wild-prior-to-public-disclosure
Critical TeamViewer Vulnerabilities Enable Code Execution Attacks Via Remote Session	https://cybersecuritynews.com/teamviewer-vulnerabilities
Cisco SD-WAN Manager Authentication 0-day Vulnerability Actively Exploited in the Wild	https://cybersecuritynews.com/cisco-sd-wan-manager-0-day-flaw
Bitget Confirms Third-Party Zero-Day Behind \$387.5 Million Cryptocurrency Theft	https://thehackernews.com/2026/10/bitget-confirms-third-party-zero-day.html
CopyEscape Docker Flaw Lets Malicious Containers Overwrite Host Files and Gain Root Access	https://cybersecuritynews.com/copyescape-docker-flaw
DIVD says Zammad zero-days enabled AI-driven network breach	https://bleepingcomputer.com/news/security/divd-says-zammad-zero-days-enabled-ai-driven-network-breach
Attackers Exploit Zimbra Flaw to Deploy Web Shells and Harvest Authentication Secrets	https://thehackernews.com/2026/09/attackers-exploit-zimbra-flaw-to-deploy.html
CISA warns of critical pre-auth RCE flaw in MikroTik RouterOS	https://bleepingcomputer.com/news/security/cisa-warns-of-critical-pre-auth-rce-flaw-in-mikrotik-routeros
Cisco Warns of Attackers Exploiting Critical Authentication Bypass in SD-WAN Manager	https://thehackernews.com/2026/09/cisco-warns-of-attackers-exploiting.html
Cisco warns of new SD-WAN zero-day exploited in attacks	https://bleepingcomputer.com/news/security/cisco-warns-of-new-sd-wan-authentication-bypass-zero-day-exploited-in-attacks
Google: AI Is Changing the Pace and Profile of Vulnerability Discovery	https://securityweek.com/google-ai-is-changing-the-pace-and-profile-of-vulnerability-discovery
AI-Found Vulnerabilities More Likely to Enable RCE, Google Says	https://infosecurity-magazine.com/news/ai-found-vulnerabilities-rce

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
Kiteworks patches max severity code injection vulnerability	https://bleepingcomputer.com/news/security/kiteworks-patches-max-severity-email-protection-gateway-code-injection-vulnerability
Cisco Patches Exploited Catalyst SD-WAN Zero-Day Vulnerability	https://securityweek.com/cisco-patches-exploited-catalyst-sd-wan-zero-day-vulnerability
Google Releases Chrome Update With 32 Security Fixes for Windows, Mac and Linux	https://cybersecuritynews.com/chrome-update-with-32-security-fixes
WatchGuard Patches Critical Firewall OS Code Injection Vulnerability	https://securityweek.com/watchguard-patches-critical-firewall-os-code-injection-vulnerability
Apple Patches CoreGraphics Zero Day Exploited in Attacks	https://infosecurity-magazine.com/news/apple-patches-coregraphics-zero
OpenSSL Fixes High-Severity DTLS Flaw That Can Leak Heap Memory Unencrypted	https://thehackernews.com/2026/09/openssl-fixes-high-severity-dtls-flaw.html
High-Severity Vulnerabilities Patched in OpenSSL, WolfSSL	https://securityweek.com/high-severity-vulnerabilities-patched-in-openssl-wolfssl

Potential threats / Threat intelligence

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

Σύντομη περιγραφή / Τίτλος	URL
Microsoft says threat actors are ahead in the early AI race	https://bleepingcomputer.com/news/security/microsoft-says-threat-actors-are-ahead-in-the-early-ai-race
Hackers Built a Windows Backdoor Whose Entire C2 Lives Inside Microsoft 365	https://cybersecuritynews.com/hackers-built-a-windows-backdoor
Fake Zoom Installer Tricks Mac Users Into Installing New CloudSyncD Backdoor	https://cybersecuritynews.com/fake-zoom-installer-tricks
WordPress Backdoor Rebuilds Itself After Cleanup Using Files, Database, and Shared Memory	https://thehackernews.com/2026/10/wordpress-backdoor-rebuilds-itself.html
Police dismantle KillSec ransomware gang allegedly led by 16-year-old	https://bleepingcomputer.com/news/security/police-dismantle-killsec-ransomware-gang-allegedly-led-by-16-year-old
Police Shut Down KillSec Ransomware, Identify Alleged Teen Leader	https://securityweek.com/police-shut-down-killsec-ransomware-identify-alleged-teen-leader
Warlock Ransomware Exploiting SharePoint Flaws to Attack Water and Telecom Operators	https://cybersecuritynews.com/warlock-ransomware-exploiting-sharepoint-flaws
CloudSyncD MacOS Backdoor Hides Behind Fake Zoom Installer	https://infosecurity-magazine.com/news/cloudsyncd-macos-backdoor-fake
Hackers Abuse Microsoft Defender Exclusions to Hide Malware From Antivirus Scans	https://cybersecuritynews.com/hackers-abuse-microsoft-defender

Treasury Blacklists Most-Wanted ATM Malware Developer and His Network	https://securityweek.com/treasury-blacklists-most-wanted-atm-malware-developer-and-his-network
Russian state hackers use new RedFlick technique to push malware	https://bleepingcomputer.com/news/security/russian-state-hackers-use-new-redflick-technique-to-push-malware
Russian Hackers Target 100+ Organizations With New RedFlick Phishing Attack	https://cybersecuritynews.com/russian-hackers-2
Phishing Response: 3 Steps SOC Teams Can Take to Investigate Threats Faster	https://cybersecuritynews.com/phishing-response-3-steps-soc-teams-can-take-to-investigate-threats-faster
Russia's Star Blizzard Ditches ClickFix to Widen Phishing Net	https://darkreading.com/threat-intelligence/russia-star-blizzard-apt-ditches-clickfix-widen-phishing-net
Attackers Combine ChatGPT Feature Abuse With ClickFix to Deliver RAT	https://infosecurity-magazine.com/news/chatgpt-feature-abuse-to-deliver

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
Δεν εντοπίστηκαν άρθρα για το καθορισμένο χρονικό διάστημα.	

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 CVSS v3.1 score ≥ 7.0 , αφορούν το διάστημα 30/09/2026–02/10/2026, 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/