

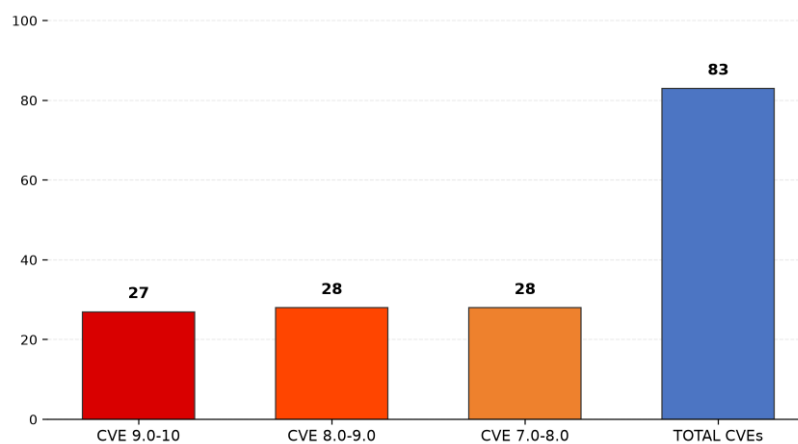


Newsletter on system vulnerabilities and cybersecurity news.

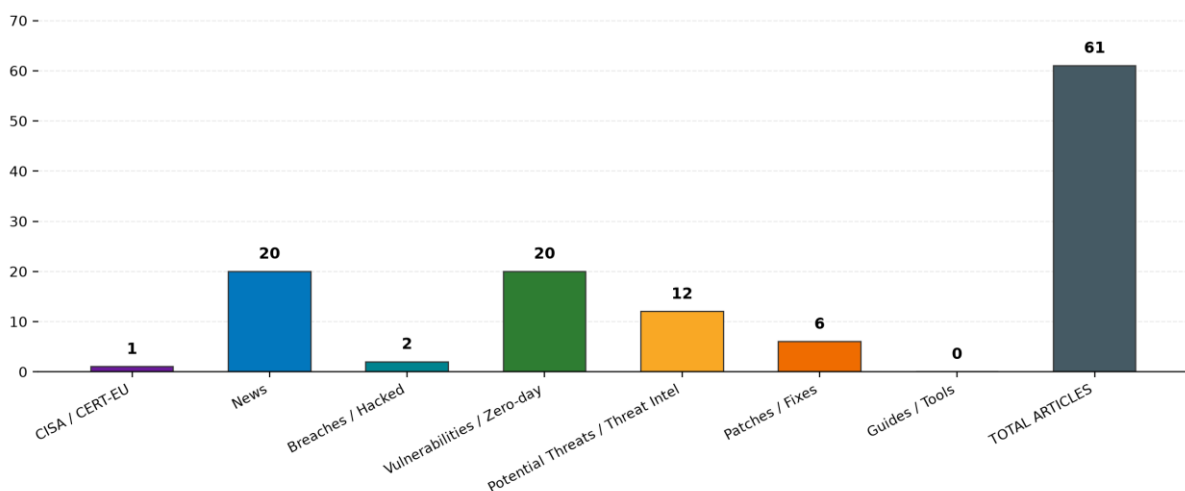
National Cyber Security Authority (NCSA)

Date: 02/09/2026 - 04/09/2026

of CVEs per CVSS score



of articles per section



Contents

Common Vulnerabilities and Exposures (CVEs)	3
CISA/CERT-EU Alerts & Advisories	12
News.....	13
Breaches / Compromised / Hacked.....	14
Vulnerabilities / Flaws / Zero-day.....	14
Patches / Updates / Fixes	15
Potential threats / Threat intelligence	16
Guides / Tools.....	16
References.....	17
Annex – Websites with vendor specific vulnerabilities	18

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-2026-70352	10,0	Azure AI Language	Missing Authentication for Critical Function		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70352			
CVE-2026-83548	10,0	the SMA1000 Appliance Work Place interface due to an unintended alternate access path	Unintended Proxy or Intermediary ('Confused Deputy'); Server-Side Request Forgery (SSRF)	versions up to (excluding) 12.4.3-03526; versions from (including) 12.5.0 up to (excluding) 12.5.0-02952	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0016	active	yes	total
CVE-2026-83711	10,0	Microsoft Azure Active Directory B2C	Authorization Bypass Through User-Controlled Key		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83711			
CVE-2026-85061	10,0	MapLibre GL JS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Prior to 6.4.1	https://github.com/maplibre/maplibre-gl-js/commit/1da69f3cd913a39fa948708e01478663bf48bc27 https://github.com/maplibre/maplibre-gl-js/pull/8189 https://github.com/maplibre/maplibre-gl-js/releases/tag/v6.4.1 https://github.com/maplibre/maplibre-gl-js/security/advisories/GHSA-jrc7-96c5-q579			
CVE-2026-85223	9,9	D-Link DNS-340L	Improper Neutralization of Special Elements used in a Command ('Command Injection'); Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	1.01B04	https://github.com/dxz0069/WAVLINK-WN530H4-Command-Injection-in-set_add_routing/blob/main/DLINK-CMD-008-vulndb.md https://vuldb.com/cve/CVE-2026-85223 https://vuldb.com/submit/894213 https://vuldb.com/vuln/398422 https://vuldb.com/vuln/398422/cti https://www.dlink.com/			
CVE-2026-11613	9,8	The Divi Ajax Filter plugin for Word-Press; all	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')	up to, and including, 5.1.2	https://diviengine.com/divi-ajax-filter-changelog/ https://www.wordfence.com/threat-intel/vulnerabilities/id/8fbb92ac-a8e7-480d-8910-416f902a2a?source=cve			
CVE-2026-82526	9,8	R2R	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	through 3.6.6	https://github.com/SciPhi-AI/R2R/issues/2309 https://www.vulncheck.com/advisories/r2r-sql-injection-via-vector-index-creation-endpoint			
CVE-2026-82923	9,8	AI Website Builder (GitHub build)		1.0.0 through 1.0.0	https://wpscan.com/vulnerability/663e7004-1cca-4c0f-8d54-7298d40fe179/			
CVE-2026-84325	9,8	DataTransfer in Google Chrome	Improper Input Validation	prior to 152.0.7977.75	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop.html	none	yes	total
CVE-2026-84372	9,8	Predis	Improper Neutralization of CRLF Sequences ('CRLF Injection')	>= 3.0.0-RC1, < 3.3.0	https://github.com/predis/predis/commit/053cb4b6ac7fb11469ead96a78d059bc0458e408 https://github.com/predis/predis/issues/1574 https://github.com/predis/predis/pull/1586 https://github.com/predis/predis/releases/tag/v3.3.0 https://github.com/predis/predis/security/advisories/GHSA-w6f5-v2h6-q786	poc	yes	total

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-84637	9,8	Thunderbird	Unrestricted Upload of File with Dangerous Type	versions up to (excluding) 153.2.0; versions from (including) 154.0 up to (excluding) 155.0	https://www.mozilla.org/security/advisories/mfsa2026-78/ https://www.mozilla.org/security/advisories/mfsa2026-88/	none	yes	total
CVE-2026-85146	9,8	SmartIT Desktop Manager developed by Lightstar has a	Use of Hard-coded Credentials	10 and earlier	https://www.twcert.org.tw/en/cp-139-11177-13ca3-2.html https://www.twcert.org.tw/tw/cp-132-11176-a4cc2-1.html			
CVE-2026-85181	9,8	CAT	Reliance on Cookies without Validation and Integrity Checking	3.1.0 and earlier	https://github.com/dianping/cat https://github.com/dianping/cat/blob/3.1.0/cat-home/src/main/java/com/dianping/cat/system/page/login/service/TokenBuilder.java https://github.com/dianping/cat/blob/3.1.0/cat-home/src/main/java/com/dianping/cat/util/HttpUtils.java https://github.com/dianping/cat/issues/2384 https://www.vulncheck.com/advisories/cat-through-3.1.0-session-cookie-forgery-via-unkeyed-hashcode-checksum	none	yes	total
CVE-2026-85504	9,8	FreeIPMI	Stack-based Buffer Overflow	before 1.6.19	https://ftp.gnu.org/gnu/freeipmi/freeipmi-1.6.19.tar.gz https://www.gnu.org/software/freeipmi/ https://www.openwall.com/lists/oss-security/2026/08/28/5			
CVE-2026-84354	9,6	FileSystem in Google Chrome	Incorrect Authorization	prior to 152.0.7977.75	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop.html	none	no	total
CVE-2026-85042	9,6	DevTools in Google Chrome	Use After Free	prior to 152.0.7977.82	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_01882797386.html https://issues.chromium.org/issues/553119925	none	no	total
CVE-2026-85047	9,6	Transactions Platform in Google Chrome on on iOS	Improper Input Validation	prior to 152.0.7977.82	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_01882797386.html https://issues.chromium.org/issues/513790581	none	no	total
CVE-2026-85050	9,6	WebGL in Google Chrome on on Android	Out-of-bounds Write	prior to 152.0.7977.82	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_01882797386.html https://issues.chromium.org/issues/549350408	none	no	total
CVE-2026-85085	9,6	The Canva Android App	Improper Verification of Source of a Communication Channel	before 2.376.0	https://trust.canva.com/?tclUId=be2ebc32-7053-4885-bf71-68771aa4589a			
CVE-2026-80098	9,3	Copilot Studio	Improper Verification of Cryptographic Signature		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-80098			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-80726	9,3	Linux		a770f6f28b1a9287189f3dc8333eb694d9a2f0a b prior to 9b7984692c18b22d6d61af3f53887fca7fddb0f1; a770f6f28b1a9287189f3dc8333eb694d9a2f0a b prior to f33ecb89d352348ed5e625f6747ac51ede254e1b; a770f6f28b1a9287189f3dc8333eb694d9a2f0a b prior to 0af4711862c5b818204d40b21f0859ad51c230e9; a770f6f28b1a9287189f3dc8333eb694d9a2f0a b prior to 66bc868a33cf1de43f22a94acd8857e0fe33393f; a770f6f28b1a9287189f3dc8333eb694d9a2f0a b prior to 9f7760a2e962cbda0d096a27d394d14ad4d22928; a770f6f28b1a9287189f3dc8333eb694d9a2f0a b prior to 5ec42d57655c690234c14aece6dd3f209778c1d8; 2.6.30	https://git.kernel.org/stable/c/0af4711862c5b818204d40b21f0859ad51c230e9 https://git.kernel.org/stable/c/5ec42d57655c690234c14aece6dd3f209778c1d8 https://git.kernel.org/stable/c/66bc868a33cf1de43f22a94acd8857e0fe33393f https://git.kernel.org/stable/c/9b7984692c18b22d6d61af3f53887fca7fddb0f1 https://git.kernel.org/stable/c/9f7760a2e962cbda0d096a27d394d14ad4d22928 https://git.kernel.org/stable/c/f33ecb89d352348ed5e625f6747ac51ede254e1b			
CVE-2026-85183	9,3	taipy	Missing Origin Validation in WebSockets	4.1.1 and earlier	https://github.com/Avaiga/taipy https://github.com/Avaiga/taipy/blob/4.1.1/taipy/quill/server.py https://github.com/Avaiga/taipy/issues/2890 https://www.vulncheck.com/advisories/taipy-through-4.1.1-cross-site-websocket-hijacking-via-wildcard-socket-io-cors	poc	no	total
CVE-2026-58400	9,1	GeoNetwork	Improper Control of Generation of Code ('Code Injection'); Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	>= 4.3.0, < 4.4.12; < 4.2.17	https://docs.geonetwork-opensource.org/4.2/overview/change-log/version-4.2.17 https://docs.geonetwork-opensource.org/4.4/overview/change-log/version-4.4.12 https://github.com/geonetwork/core-geonetwork/security/advisories/GHSA-x898-729x-cc3r https://thehackernews.com/2026/09/geonetwork-fixes-unauthenticated-rce.html			
CVE-2026-62916	9,1	Microsoft Entra ID	Authentication Bypass Using an Alternate Path or Channel		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62916			
CVE-2026-84479	9,1	AVideo	Authentication Bypass by Spoofing	29.0 and earlier	https://github.com/MWBN/AVideo/security/advisories/GHSA-m9m3-qwh2-337c https://www.vulncheck.com/advisories/mwbn-avideo-authentication-bypass-via-user-agent-header	poc	yes	partial

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-75604	9,0	next.js	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	>= 13.4.0, < 15.5.24; >= 16.0.0, < 16.3.3	https://github.com/vercel/next.js/commit/968b9fcb26bdeb8e0a861a9df05361474666d51b https://github.com/vercel/next.js/commit/b0f3460a92b955d3ca41fccf9a525a2b910fbf3 https://github.com/vercel/next.js/releases/tag/v15.5.24 https://github.com/vercel/next.js/releases/tag/v16.3.3 https://github.com/vercel/next.js/security/advisories/GHSA-p293-qw3h-ir36	none	no	total
CVE-2026-84324	9,0	Proxy in Google Chrome	Use After Free	prior to 152.0.7977.75	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop.html	none	no	total
CVE-2026-71963	8,8	Hermes Agent	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	0.18.2 through 0.21.0	https://github.com/NousResearch/hermes-agent/commit/f6234d00c5d59450adea1d7edd30ad3859375c79 https://github.com/NousResearch/hermes-agent/pull/101483 https://www.manifold.security/blog/ai-coding-agents-git-hijack https://www.vulncheck.com/advisories/hermes-agent-rce-via-git-core-fsmonitor-config-injection	poc	no	total
CVE-2026-84326	8,8	V8 in Google Chrome	Use of Uninitialized Resource	prior to 152.0.7977.75	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop.html	none	no	total
CVE-2026-84347	8,8	WebRTC in Google Chrome	Use After Free	prior to 152.0.7977.75	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop.html	none	no	total
CVE-2026-84350	8,8	TabStrip in Google Chrome	Use After Free	prior to 152.0.7977.75	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop.html	none	no	total
CVE-2026-84482	8,8	WWBN AVideo through commit; the get_domain() and isSameDomain() functions that fail to properly validate referer origins	Origin Validation Error	9c39d8c8b4c1f75540788d6b391740852ceb0732 and earlier	https://github.com/WWBN/AVideo/security/advisories/GHSA-jm6j-xqvg-r8p5 https://www.vulncheck.com/advisories/wwbn-avideo-cross-site-request-forgery-via-get-domain-validation	poc	no	total
CVE-2026-85049	8,8	Skia in Google Chrome	Use After Free	prior to 152.0.7977.82	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_01882797386.html https://issues.chromium.org/issues/553345874	none	no	total
CVE-2026-85051	8,8	Compositing in Google Chrome	Access of Resource Using Incompatible Type ('Type Confusion')	prior to 152.0.7977.82	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_01882797386.html https://issues.chromium.org/issues/553449113	none	no	total
CVE-2026-85053	8,8	CacheStorage in Google Chrome	Exposure of Resource to Wrong Sphere	prior to 152.0.7977.82	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_01882797386.html https://issues.chromium.org/issues/552689418	none	no	total
CVE-2026-85174	8,8	SiYuan	Insertion of Sensitive Information into Log File	before v3.8.2	https://github.com/siyuan-note/siyuan/security/advisories/GHSA-3wvc-5754-gp67 https://www.vulncheck.com/advisories/siyuan-before-3.8.2-api-token-exposure-via-log-file			
CVE-2026-85175	8,8	SiYuan versions	Files or Directories Accessible to External Parties	<= 3.8	https://github.com/siyuan-note/siyuan/security/advisories/GHSA-4wwp-f6qw-6qm5 https://www.vulncheck.com/advisories/siyuan-before-3.8.2-tls-private-key-disclosure-via-getfile	poc	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-2026-85176	8,8	the jsldata controller, allowing authenticated users to read and write arbitrary files via file:// scheme resolution	External Control of File Name or Path	7.2.6 and earlier	https://github.com/dbgate/dbgate https://github.com/dbgate/dbgate/blob/v7.2.6/packages/api/src/controllers/jsldata.js https://github.com/dbgate/dbgate/blob/v7.2.6/packages/api/src/utility/getJsFileName.js https://github.com/dbgate/dbgate/issues/1502 https://www.vulncheck.com/advisories/dbgate-through-7.2.6-arbitrary-file-read-and-write-via-file-isdid	none	no	total
CVE-2026-85452	8,8	MOOS ui-moos; ScopeTabPage	Out-of-bounds Write	through 50b9c6c	https://github.com/themoos/ui-moos https://github.com/themoos/ui-moos/blob/50b9c6c65169c501f746cfef1e167f74a7735e74/Tools/Graphical/uMS/ScopeTabPage.cpp#L243 https://github.com/themoos/ui-moos/commit/a6ebc0bc6cb360315ce620e865f996d189cddb0e https://github.com/themoos/ui-moos/pull/5 https://www.vulncheck.com/advisories/moos-ui-moos-through-50b9c6c-ums-buffer-overflow-via-long-moos-identifiers			
CVE-2026-85540	8,8	DreamMaker	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	all	https://www.twcert.org.tw/en/cp-139-11184-9ad14-2.html https://www.twcert.org.tw/tw/cp-132-11183-06a5e-1.html			
CVE-2026-71404	8,7	Rancher Manager	Authorization Bypass Through User-Controlled Key	before 2.15.1.	https://github.com/rancher/rancher/pull/56593 https://github.com/rancher/rancher/pull/56642	none	no	total
CVE-2026-80465	8,7	Mendix SAML (Mendix)	Improper Verification of Cryptographic Signature	< V4.2.3); < V3.6.27)	https://cert-portal.siemens.com/productcert/html/ssa-887643.html	none	no	total
CVE-2026-65818	8,5	Power Automate	Server-Side Request Forgery (SSRF)		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65818			
CVE-2026-69857	8,5	Azure Cosmos DB	Authorization Bypass Through User-Controlled Key		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69857			
CVE-2026-70178	8,5	Microsoft Fabric	Missing Authorization		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70178			
CVE-2026-84349	8,3	Browser in Google Chrome	Use After Free	prior to 152.0.7977.75	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop.html	none	no	total
CVE-2026-84351	8,3	GPU in Google Chrome on Windows	Stack-based Buffer Overflow	prior to 152.0.7977.75	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop.html	none	no	total
CVE-2026-63376	8,2	toml-node	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	Prior to 4.1.2	https://github.com/BinaryMuse/toml-node/commit/def6ab5ea99038c0dd482cd6af1745a6af8b4c44 https://github.com/BinaryMuse/toml-node/commit/d1aff662276adc38a2e03df3139f7119b0185463 https://github.com/BinaryMuse/toml-node/security/advisories/GHSA-v5mp-igw5-2x6j			
CVE-2026-84370	8,2	SVGO, short for SVG Optimizer	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'); Incomplete List of Disallowed Inputs	>= 1.0.0, < 2.8.4; >= 3.0.0, < 3.3.5; >= 4.0.0, < 4.1.0	https://github.com/svg/svgo/commit/0557385564a5c6c11d76cd934a6cff94451e532c https://github.com/svg/svgo/commit/3db3ef33e409a0bc0fdaf255e46c908b00e93bc2 https://github.com/svg/svgo/commit/994a9f00d79ddec68ce19a1ce9eb8ca08d747e4f https://github.com/svg/svgo/pull/2268 https://github.com/svg/svgo/pull/2269 https://github.com/svg/svgo/pull/2272	none	no	partial

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-84696	8,2	PS3111-S11 Controller Firmware	Missing Authentication for Critical Function	SBFQT1.3	https://github.com/trulycrisp/disksec https://github.com/trulycrisp/psychite https://trulycrisp.github.io/drivefirmware/phison_s11/ https://www.vulncheck.com/advisories/phison-ps3111-s11-controller-firmware-missing-authentication-on-vendor-unique-commands	poc	no	total
CVE-2026-78583	8,1	Kibana	Incorrect Authorization	8.0.0 through 8.19.20; 9.0.0 through 9.4.5; 9.5.0 through 9.5.2	https://discuss.elastic.co/t/kibana-8-19-21-9-4-6-9-5-3-security-update-esa-2026-140/390158	none	no	total
CVE-2026-84334	8,1	Chromoting in Google Chrome on Windows	Incorrect Authorization	prior to 152.0.7977.75	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop.html	none	no	total
CVE-2026-85160	8,1	AVideo through commit c91b5975d	External Control of File Name or Path	c91b5975d and earlier	https://github.com/WWBN/AVideo/security/advisories/GHSA-qghx-ccvr-97q7 https://www.vulncheck.com/advisories/avideo-through-c91b5975d-csrf-and-path-traversal-via-stoplive-php	poc	no	total
CVE-2026-85214	8,1	vhr	Authorization Bypass Through User-Controlled Key	03abbd35af24e55368ce4e09f4038dc2aba3ff5f and earlier	https://github.com/lenve/vhr https://github.com/lenve/vhr/blob/03abbd35af24e55368ce4e09f4038dc2aba3ff5f/vhr/vhrserver/vhr-mapper/src/main/java/org/javaboy/vhr/mapper/HrMapper.xml https://github.com/lenve/vhr/blob/03abbd35af24e55368ce4e09f4038dc2aba3ff5f/vhr/vhrserver/vhr-web/src/main/java/org/javaboy/vhr/controller/HrInfoController.java https://github.com/lenve/vhr/issues/349 https://www.vulncheck.com/advisories/vhr-missing-authorization-in-put-hr-info-allows-arbitrary-profile-overwrite	poc	no	partial
CVE-2026-85388	8,1	Worklenz	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	through 3.0.0	https://github.com/Worklenz/worklenz https://github.com/Worklenz/worklenz/blob/v3.0.0/worklenz-backend/src/controllers/job-titles-controller.ts https://github.com/Worklenz/worklenz/blob/v3.0.0/worklenz-backend/src/controllers/worklenz-controller-base.ts https://github.com/Worklenz/worklenz/issues/395 https://github.com/Worklenz/worklenz/security/advisories/GHSA-f2f8-2pgj-85pf https://www.vulncheck.com/advisories/worklenz-through-3.0.0-sql-injection-via-the-sort-field-query-parameter	poc	no	total
CVE-2026-64195	7,8	There; DASyLab due to lack of proper validation of user-supplied data	Out-of-bounds Write	all versions before 2026.0.0.	https://www.measx.com/en/service/productsecurity/security-updates-for-measx-software/159-securityupdates/1071-out-of-bounds-write-vulnerabilities-in-dasylab-2.html			
CVE-2026-76642	7,8	util-linux versions	Detection of Error Condition Without Action	through 2.41.5	https://github.com/util-linux/util-linux https://github.com/util-linux/util-linux/blob/v2.42.2/libmount/src/context_mount.c#L476 https://github.com/util-linux/util-linux/blob/v2.42.2/libmount/src/context_mount.c#L892 https://github.com/util-linux/util-linux/commit/1d14676ea70003e9f5b2a6a76af0cadb1190411a https://github.com/util-linux/util-linux/commit/a15c00a9e545aa8b9cf6ec0f888ff6c7b3eaeedc https://github.com/util-linux/util-linux/commit/f57cea130839c0af8dc0525274267ae4cfd66bbf	poc	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-2026-83549	7,8	SMA1000	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	versions up to (excluding) 12.4.3-03526; versions from (including) 12.5.0 up to (excluding) 12.5.0-02952	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0016	active	no	total
CVE-2026-83959	7,8	Substance3D - Sampler; arbitrary code execution in the context of the current user	Heap-based Buffer Overflow	6.0.1 and earlier	https://helpx.adobe.com/security/products/substance3d-sampler/apsb26-121.html			
CVE-2026-85028	7,8	a directory with insecure permissions in the FPGA management tool installation component in AWS FPGA Development Kit (aws-fpga)	Creation of Temporary File in Directory with Insecure Permissions	before 2.3.4	https://aws.amazon.com/security/security-bulletins/2026-096-aws/ https://github.com/aws/aws-fpga/releases/tag/v2.3.4 https://github.com/aws/aws-fpga/security/advisories/GHSA-q4hc-wrmm-2x74	none	no	total
CVE-2026-55658	7,7	Gardens	Missing Authorization	<= 3e595f3	https://github.com/1Hive/gardens-v2/security/advisories/GHSA-jwvq-5xmf-f377			
CVE-2026-85178	7,7	helicone	Authorization Bypass Through User-Controlled Key	prior to ca34549ea56f7ed587843f82d9cc19baa1f36ba4	https://github.com/Helicone/helicone https://github.com/Helicone/helicone/commit/ca34549ea56f7ed587843f82d9cc19baa1f36ba4 https://github.com/Helicone/helicone/issues/5712 https://www.vulncheck.com/advisories/helicone-cross-tenant-provider-key-disclosure-via-missing-organization-filter	poc	no	partial
CVE-2026-85211	7,7	proxy_api	Authorization Bypass Through User-Controlled Key	1.23.0 and earlier	https://github.com/HumanSignal/label-studio https://github.com/HumanSignal/label-studio/blob/1.23.0/label_studio/io_storages/proxy_api.py https://github.com/HumanSignal/label-studio/issues/9924 https://www.vulncheck.com/advisories/label-studio-through-1.23.0-cross-organization-storage-uri-resolution	poc	no	partial
CVE-2026-53635	7,6	openedx-platform	Missing Authorization	< 59bb6d669e4fdc24d96afb809e12119372d9e257	https://github.com/openedx/openedx-platform/commit/59bb6d669e4fdc24d96afb809e12119372d9e257 https://github.com/openedx/openedx-platform/commit/f25bbc4d52bd827c8f04c73de427e2e16a144c73 https://github.com/openedx/openedx-platform/commit/fd93ef5f9940f4ad6f50cf7faecad8d9cf2d3336 https://github.com/openedx/openedx-platform/security/advisories/GHSA-rqg6-w4pv-7piv	poc	no	partial
CVE-2026-57777	7,6	WooCommerce	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	before 11.0.	https://github.com/woocommerce/woocommerce/pull/67554 https://patchstack.com/database/wordpress/plugin/woocommerce/vulnerability/wordpress-woocommerce-plugin-10-9-4-sql-injection-vulnerability?_s_id=cve			
CVE-2026-85197	7,6	libsoup	Use After Free		https://access.redhat.com/security/cve/CVE-2026-85197 https://bugzilla.redhat.com/show_bug.cgi?id=2528425			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-85213	7,6	Kill Bill	Missing Authorization	through 0.24.21	https://github.com/killbill/killbill https://github.com/killbill/killbill/blob/killbill-0.24.21/jaxrs/src/main/java/org/killbill/billing/jaxrs/resources/AdminResource.java https://github.com/killbill/killbill/issues/2251 https://www.vulncheck.com/advisories/kill-bill-through-0.24.21-missing-authorization-on-adminresource-endpoints	none	no	partial
CVE-2026-76169	7,5	fastify	Authentication Bypass Using an Alternate Path or Channel	>= 4.0; before 5.12.2; 5.12.2 or later	https://cna.openjsf.org/security-advisories.html https://github.com/fastify/fastify/security/advisories/GHSA-p68g-wchp-6fh7			
CVE-2026-81665	7,5	Corosync's Totem Process Group (to-tempg) message reassembly	Heap-based Buffer Overflow		https://access.redhat.com/security/cve/CVE-2026-81665 https://bugzilla.redhat.com/show_bug.cgi?id=2524910			
CVE-2026-82520	7,5	parsedmarc	Improper Handling of Highly Compressed Data (Data Amplification)	before 11.0.1	https://github.com/domainaware/parsedmarc/releases/tag/11.0.1 https://github.com/domainaware/parsedmarc/security/advisories/GHSA-43qf-f35w-2x4r https://www.vulncheck.com/advisories/parsedmarc-zip-bomb-dos-via-compressed-email-attachments			
CVE-2026-84485	7,5	APITable	Missing Authentication for Critical Function	through 1.13.0-beta.1	https://github.com/apitable/apitable https://github.com/apitable/apitable/blob/88b24ce9f359cc434778be75d03603182882dc76/backend-server/application/src/main/java/com/apitable/internal/controller/InternalOrganizationController.java#L58 https://github.com/apitable/apitable/blob/88b24ce9f359cc434778be75d03603182882dc76/backend-server/application/src/main/java/com/apitable/shared/context/LoginContext.java https://github.com/apitable/apitable/blob/88b24ce9f359cc434778be75d03603182882dc76/backend-server/application/src/main/java/com/apitable/shared/interceptor/ResourceInterceptor.java#L85 https://www.vulncheck.com/advisories/apitable-through-1.13.0-beta.1-missing-authentication-on-the-internal-organization-load-or-search-endpoint	none	yes	partial
CVE-2026-85182	7,5	PUT /hr/pass requests belongs to the authenticated caller	Authorization Bypass Through User-Controlled Key	03abbd35af24e55368ce4e09f4038dc2aba3ff5f and earlier	https://github.com/lenve/vhr https://github.com/lenve/vhr/blob/03abbd35af24e55368ce4e09f4038dc2aba3ff5f/vhr/vhrserver/vhr-service/src/main/java/org/javaboy/vhr/service/HrService.java https://github.com/lenve/vhr/blob/03abbd35af24e55368ce4e09f4038dc2aba3ff5f/vhr/vhrserver/vhr-web/src/main/java/org/javaboy/vhr/controller/HrInfoController.java https://github.com/lenve/vhr/issues/350 https://www.vulncheck.com/advisories/vhr-missing-authorization-in-put-hr-pass-allows-cross-account-password-change	poc	no	total
CVE-2026-85393	7,5	node-forge	Improper Verification of Cryptographic Signature	through 1.4.0	https://github.com/advisories/GHSA-ppp5-5v6c-4iwp https://github.com/digitalbazaar/forge https://github.com/digitalbazaar/forge/blob/v1.4.0/lib/asn1.js https://github.com/digitalbazaar/forge/blob/v1.4.0/lib/rsa.js https://github.com/digitalbazaar/forge/issues/1149 https://www.vulncheck.com/advisories/node-forge-through-1.4.0-rsa-pkcs-1-1.5-signature-forgery-via-nested-digestalgorithm-padding	poc	yes	partial

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-85396	7,5	rubyzip versions	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	versions before 3.4.0	https://github.com/geo-chen/oss/blob/main/rubyzip.md https://github.com/rubyzip/rubyzip https://github.com/rubyzip/rubyzip/blob/v3.3.1/lib/zip/entry.rb https://github.com/rubyzip/rubyzip/commit/17edfb4423b83211b075acc23a7d8640da63449 https://github.com/rubyzip/rubyzip/releases/tag/v3.4.0 https://www.vulncheck.com/advisories/rubyzip-before-3.4.0-path-traversal-in-zip-entry-extract-via-sibling-directory-prefix	none	yes	partial
CVE-2026-85429	7,5	MOOS-IvP uFldNodeComms	Insufficient Verification of Data Authenticity	through 24.8.1	https://github.com/moos-ivp/moos-ivp https://github.com/moos-ivp/moos-ivp/blob/1de9ae146cd63c209e8c3fd81611a4ed2472971b/ivp/src/uFldNodeComms/FldNodeComms.cpp#L114 https://github.com/moos-ivp/moos-ivp/commit/3907ac07cdfd8a7255d65657dc18dc6b77b30b64 https://github.com/moos-ivp/moos-ivp/pull/122 https://www.vulncheck.com/advisories/moos-ivp-through-24.8.1-ufldnodecomms-node-message-source-spoofing			
CVE-2026-85446	7,5	MOOS-IvP versions	Inefficient Algorithmic Complexity	through 24.8.1	https://github.com/moos-ivp/moos-ivp https://github.com/moos-ivp/moos-ivp/blob/1de9ae146cd63c209e8c3fd81611a4ed2472971b/ivp/src/uFldNodeComms/FldNodeComms.cpp#L169 https://github.com/moos-ivp/moos-ivp/commit/8e30008d4eb68d83797187bd46e929e6cb06b195 https://github.com/moos-ivp/moos-ivp/pull/131 https://www.vulncheck.com/advisories/moos-ivp-through-24.8.1-ufldnodecomms-quadratic-processing-denial-of-service			
CVE-2026-85447	7,5	MOOS-IvP pRealm	Allocation of Resources Without Limits or Throttling	through version 24.8.1	https://github.com/moos-ivp/moos-ivp https://github.com/moos-ivp/moos-ivp/blob/1de9ae146cd63c209e8c3fd81611a4ed2472971b/ivp/src/pRealm/PipeWay.cpp#L109 https://github.com/moos-ivp/moos-ivp/commit/8a4bb9d9154a70e769a7290ee11dde5157c03e9b https://github.com/moos-ivp/moos-ivp/pull/132 https://www.vulncheck.com/advisories/moos-ivp-through-24.8.1-prealm-unbounded-realmcast-req-subscription-denial-of-service			
CVE-2026-85449	7,5	MOOS-IvP pMarineViewer	Allocation of Resources Without Limits or Throttling	through 24.8.1	https://github.com/moos-ivp/moos-ivp https://github.com/moos-ivp/moos-ivp/blob/1de9ae146cd63c209e8c3fd81611a4ed2472971b/ivp/src/lib_geodaid/ContactLedger.cpp#L186 https://github.com/moos-ivp/moos-ivp/commit/4d8d0693d3f8bf8907dc0aed04ea488d85af9f22 https://github.com/moos-ivp/moos-ivp/pull/134 https://www.vulncheck.com/advisories/moos-ivp-through-24.8.1-pmarineviewer-unbounded-memory-consumption-via-node-report			
CVE-2026-8862	7,5	IBM Netezza Software	Insufficiently Protected Credentials	11.3.0.3 through Interim Fix 002	https://www.ibm.com/support/pages/node/7284359			
CVE-2026-62906	7,4	data query logic in Microsoft Discovery Studio	Improper Neutralization of Special Elements in Data Query Logic		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62906			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-85525	7,4	the Snowflake Python, Go, JDBC, and Node	Improper Certificate Validation; Improper Verification of Cryptographic Signature	prior to 4.7.3; prior to 2.2.0; prior to 4.3.4; prior to 3.3.0	https://docs.snowflake.com/en/release-notes/clients-drivers/golang-2026 https://docs.snowflake.com/en/release-notes/clients-drivers/jdbc-2026 https://docs.snowflake.com/en/release-notes/clients-drivers/nodejs-2026 https://github.com/snowflakedb/snowflake-connector-python/releases/tag/v4.7.3			
CVE-2026-78590	7,3	the Kibana Fleet feature	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	versions from (including) 8.0.0 up to (excluding) 8.19.18; versions from (including) 9.0.0 up to (excluding) 9.3.6; versions from (including) 9.4.0 up to (excluding) 9.4.3	https://discuss.elastic.co/t/kibana-8-19-18-9-3-6-9-4-3-security-update-esa-2026-158/390113	none	no	partial
CVE-2026-85390	7,1	Checkmate	Missing Authorization	through 3.11.0	https://github.com/bluewave-labs/Checkmate https://github.com/bluewave-labs/Checkmate/blob/v3.11.0/server/src/api/routes/checkRoutes.ts https://github.com/bluewave-labs/Checkmate/blob/v3.11.0/server/src/api/routes/maintenanceWindowRoutes.ts https://github.com/bluewave-labs/Checkmate/blob/v3.11.0/server/src/api/routes/notificationRoutes.ts https://github.com/bluewave-labs/Checkmate/issues/3916 https://www.vulncheck.com/advisories/checkmate-through-3.11.0-missing-authorization-on-maintenance-window-notification-and-check-deletion-routes			

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 Seven Known Exploited Vulnerabilities to Catalog CISA	CISA has added seven new vulnerabilities to its KEV Catalog, based on evidence of active exploitation.	https://cisa.gov/news-events/alerts/2026/09/02/cisa-adds-seven-known-exploited-vulnerabilities-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
Microsoft Teams to Add QR Code Protection in Teams Messaging	https://cybersecuritynews.com/microsoft-teams-qr-code-protection
OpenAI Pledges \$1bn to Bring its AI Cybersecurity Tools to Essential S	https://infosecurity-magazine.com/news/openai-pledges-ai-tools-essential
G7 Urges Fast-Track on Quantum-Safe Cybersecurity Rules	https://infosecurity-magazine.com/news/g7-urges-quantum-safe-cyber-rules
GPT-6 Astra Scores 100% on ExploitBench as OpenAI Blocks PoC Exploit Requests	https://thehackernews.com/2026/09/gpt-6-astra-scores-100-on-exploitbench.html
LLMjacking Attack Uses Leaked AWS IAM Key to Steal Paid AI Model Access	https://cybersecuritynews.com/llmjacking-attack
Fewer attacks, more force: Link11's European Cyber Report finds new DDoS records for the first half of 2026	https://cybersecuritynews.com/fewer-attacks-more-force-link11s-european-cyber-report-finds-new-ddos-records-for-the-first-half-of-2026
Manchester Airports Group Data on 8.8 Million People Leaked After Ransom Refusal	https://securityweek.com/manchester-airports-group-data-on-8-8-million-people-leaked-after-ransom-refusal
Pegasus Zero-Click Exploit Infects Serbian Student Activist's iPhone	https://infosecurity-magazine.com/news/pegasus-zero-click-exploit
Microsoft: KB5120998 mouse reset bug affects only non-English PCs	https://bleepingcomputer.com/news/microsoft/microsoft-kb5120998-mouse-reset-bug-affects-only-non-english-pcs
Capsule Security Launches 'AI Circuit Breaker' to Stop Rogue Agents	https://securityweek.com/capsule-security-launches-ai-circuit-breaker-to-stop-rogue-agents
OpenAI confirms ChatGPT is down ahead of 'Astra' model launch	https://bleepingcomputer.com/news/artificial-intelligence/openai-confirms-chatgpt-is-down-ahead-of-astra-model-launch
OpenAI Investigates Elevated Errors Affecting ChatGPT and Codex Services	https://cybersecuritynews.com/openai-investigates-elevated-errors
Anthropic confirms Claude is down, multiple models affected	https://bleepingcomputer.com/news/artificial-intelligence/anthropic-confirms-claude-is-down-multiple-models-affected
Phantom Deal Hackers Impersonate Executives and Use Fake NDAs to Steal Corporate Wire Transfers	https://cybersecuritynews.com/phantom-deal-hackers
Claude AI Faces Outage Impacting Mythos 5.1, Fable 5.1, and Opus 5	https://cybersecuritynews.com/claude-ai-faces-outage
AI 'Machine Speed' Cuts 2-Week Attack Down to 10 Hours	https://darkreading.com/cyberattacks-data-breaches/ai-machine-speed-2-week-attack-10-hours
New \$7 SweepLED Device That Allows Anyone to Detect Hidden Cameras in Hotels	https://cybersecuritynews.com/sweepled-gadget
CREST Onboards First Cohort for AI-Enabled Pentesting Accreditation	https://infosecurity-magazine.com/news/crest-first-cohort-ai-pentesting
HiddenLayer Raises \$100 Million for AI Runtime Security	https://securityweek.com/hiddenlayer-raises-100-million-for-ai-runtime-security
Microsoft says KB5120998 Windows update resets desktop settings	https://bleepingcomputer.com/news/microsoft/microsoft-says-kb5120998-windows-update-resets-desktop-settings

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
French hospital fined €500,000 after breach exposes data of 727,000	https://bleepingcomputer.com/news/security/french-hospital-fined-500-000-after-breach-exposes-data-of-727-000
Coder's registry infrastructure compromised to push malicious modules	https://bleepingcomputer.com/news/security/coders-registry-infrastructure-compromised-to-push-malicious-modules

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
Over 440,000 Exploit Attempts Target Super Forms and Elementor Pro RCE Flaws	https://thehackernews.com/2026/09/over-440000-exploit-attempts-target.html
Google Releases Chrome Update to Patch Actively Exploited V8 Zero-Day	https://thehackernews.com/2026/09/google-releases-chrome-update-to-patch.html
Critical Chrome 0-Day Vulnerability Actively Exploited in the Wild	https://cybersecuritynews.com/chrome-0-day-flaw-exploited-wild
OpenAI GPT-6 Astra Discovers Zero-Day Flaws and Builds Working Exploits in Cyber Tests	https://cybersecuritynews.com/openai-gpt-6-astra-discovers-zero-day
Critical Cisco Nexus 9000 Flaw Lets Unauthenticated Remote Attackers Run Code as Root	https://thehackernews.com/2026/09/critical-cisco-nexus-9000-flaw-lets.html
Critical Elementor Pro flaw exploited to take over WordPress sites	https://bleepingcomputer.com/news/security/critical-elementor-pro-flaw-exploited-to-take-over-wordpress-sites
Chaotic Eclipse Claims Avast Antivirus 0-Day Vulnerability - PoC Released	https://cybersecuritynews.com/avast-antivirus-0-day-vulnerability-poc-released
Critical VMware Workstation and Fusion Vulnerabilities Allow Attackers to Execute Code on the Host	https://cybersecuritynews.com/vmware-workstation-and-fusion-vulnerabilities
Plex warns users to patch security vulnerabilities immediately	https://bleepingcomputer.com/news/security/plex-warns-users-to-patch-security-vulnerabilities-immediately
Over 3 Million WordPress Sites Affected by Migration Plugin Vulnerability	https://securityweek.com/over-3-million-wordpress-sites-affected-by-migration-plugin-vulnerability
Cisco Nexus 9000 Series Switches Flaw Allows Remote Attackers to Execute Malicious Code	https://cybersecuritynews.com/cisco-nexus-9000-series-switches-vulnerability
Researcher Releases FalconFlank PoC Showing Privilege Escalation in CrowdStrike Falcon	https://thehackernews.com/2026/09/researcher-releases-falconflank-poc.html
Researcher Claims CrowdStrike Falcon 0-Day Privilege Escalation Vulnerability	https://cybersecuritynews.com/crowdstrike-falcon-0-day
CISA Adds Seven Exploited Flaws as Attackers Deploy Reverse Shells and Crypto Miners	https://thehackernews.com/2026/09/cisa-adds-seven-exploited-flaws-as.html

Σύντομη περιγραφή / Τίτλος	URL
AI's Vulnerability Surge May Be More Manageable Than Feared	https://darkreading.com/application-security/ai-vulnerability-surge-manageable-than-first-feared
Hackers exploit Sangoma Switchvox flaw to deploy reverse shells	https://bleepingcomputer.com/news/security/hackers-exploit-sangoma-switchvox-flaw-to-deploy-reverse-shells
Critical SonicWall SMA 1000 Flaws Enable Unauthenticated RCE	https://darkreading.com/vulnerabilities-threats/sonicwall-sma-1000-zero-days-unauthenticated-rce
WordPress backup plugin flaw exposes millions of sites to takeover attacks	https://bleepingcomputer.com/news/security/wordpress-backup-plugin-flaw-exposes-millions-of-sites-to-takeover-attacks
GitSpawn Flaws Let Malicious Repositories Execute Code in Claude Code, Codex, Cursor, and Grok	https://cybersecuritynews.com/gitspawn-flaws-execute-code
Hackers exploit critical JFrog Artifactory flaw to forge admin tokens	https://bleepingcomputer.com/news/security/hackers-exploit-critical-jfrog-artifactory-flaw-to-forge-admin-tokens

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
Plex Urges Immediate Updates After Patching Multiple Undisclosed Security Flaws	https://thehackernews.com/2026/09/plex-urges-immediate-updates-after.html
HPE patches critical ArubaOS-CX remote code execution flaw	https://bleepingcomputer.com/news/security/hpe-patches-critical-arubaos-cx-remote-code-execution-flaw
Cisco Warns of Unpatched Secure Email Flaws, Patches Critical Switch Vulnerabilities	https://securityweek.com/cisco-warns-of-unpatched-secure-email-flaws-patches-critical-switch-vulnerabilities
Rockwell Automation Patches Over a Dozen Vulnerabilities Across Products	https://securityweek.com/rockwell-automation-patches-over-a-dozen-vulnerabilities-across-products
GeoNetwork Fixes Unauthenticated RCE Chain Affecting Government Geoportal Backends	https://thehackernews.com/2026/09/geonetwork-fixes-unauthenticated-rce.html
Unpatched Flaws Grant Access to Philippines Nuclear Agency	https://darkreading.com/cyberattacks-data-breaches/old-unpatched-flaws-attackers-philippines-nuclear-agency

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
14 Fake macOS Installers Linked to DPRK Campaign Deliver Credential-Stealing RAT	https://cybersecuritynews.com/14-fake-macos-installers
Dahua Camera Backdoor Survives Password Changes and Factory Resets on Compromised Devices	https://cybersecuritynews.com/dahua-camera-backdoor
Botnet Takedowns Are Working — But DDoS Operators Are Already Adapting	https://cybersecuritynews.com/botnet-takedowns-are-working-but-ddos-operators-are-already-adapting
ThreatsDay: CEO Phishing Kits, 5K Dropbox Account Hacks, OAuth Traps + 17 More Stories	https://thehackernews.com/2026/09/threatsday-ceo-phishing-kits-5k-dropbox.html
Hackers Weaponize ScreenConnect to Spread Worm-Like Malware Across Windows Systems	https://cybersecuritynews.com/hackers-weaponize-screenconnect
Outsider Phishing Kit Survives Takedown With 700 New Pages	https://infosecurity-magazine.com/news/outsider-phishing-kit-survives
The Gentlemen Ransomware Hackers Disable EDR and Backups Before Encrypting Networks in Under 24 Hours	https://cybersecuritynews.com/the-gentlemen-ransomware
International Operation Disrupts Salty P2P Botnet	https://infosecurity-magazine.com/news/international-operation-disrupts
VPN Is the Biggest Backdoor Into Your Plant — Here's What Should Replace It on Your OT Network	https://cybersecuritynews.com/vpn-is-the-biggest-backdoor-into-your-plant-heres-what-should-replace-it-on-your-ot-net-work
Russian Man Extradited Over Malware Campaign Targeting Freelancers	https://infosecurity-magazine.com/news/russian-man-extradited-malware
Ransomware Hackers Use New TukTuk Malware to Steal Credentials and Disable Security Tools	https://cybersecuritynews.com/new-tuktuk-malware
Attackers Exploit Two SonicWall SMA 1000 Zero-Days That May Form an Attack Chain	https://thehackernews.com/2026/09/attackers-exploit-two-sonicwall-sma.html

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 02/09/2026–04/09/2026, εντοπίστηκαν 138 επιλέξιμα CVEs και καταγράφονται 83, με κανόνα $\text{floor}(70 + 0.20 \times (N - 70))$ και αναλογική κατανομή στις ζώνες CVSS 9,0–10,0, 8,0–9,0 και 7,0–8,0.

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/