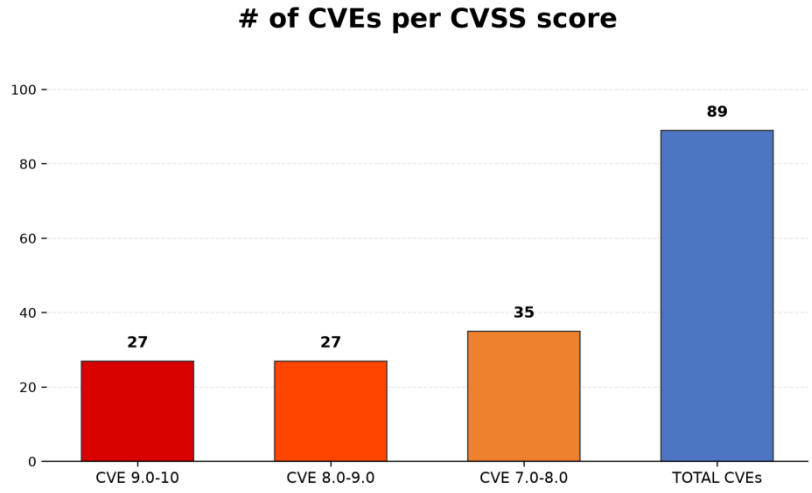
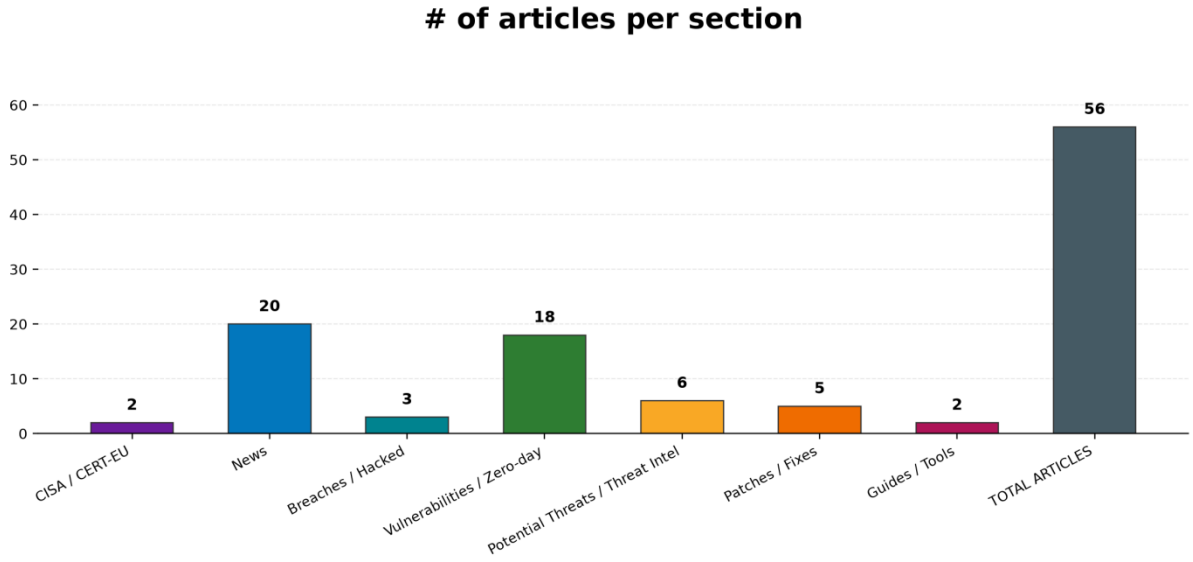
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 10/10/2026 - 13/10/2026





Contents

Common Vulnerabilities and Exposures (CVEs) 3
CISA/CERT-EU Alerts & Advisories 15
News 15
Breaches / Compromised / Hacked 16
Vulnerabilities / Flaws / Zero-day 16
Patches / Updates / Fixes 17
Potential threats / Threat intelligence 18
Guides / Tools 18
References 19
Annex – Websites with vendor specific vulnerabilities 20

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-2024-34323	10,0	ProPhoenix Law RMS	Authorization Bypass Through User-Controlled Key		https://prophoenix.com/law-rms/ https://sedriclouissaint.com/blog/prophoenix-law-rms-authentication-bypass-cve-2024-34323/#cve-details	none	yes	total
CVE-2026-103849	10,0	Adobe Commerce	Improper Neutralization of Special Elements Used in a Template Engine	2.4.9-2026-sep, 2.4.8-2026-sep, 2.4.7-2026-sep, 2.4.6-2026-sep, 2.4.5-2026-sep, 2.4.4-2026-sep and earlier; 1.5.3-2026-sep, 1.5.2-2026-sep, 1.4.2-2026-sep, 1.3.4-2026-sep, 1.3.3-2026-sep and earlier; 2.4.9-2026-sep, 2.4.8-2026-sep, 2.4.7-2026-sep and earlier	https://www.adobe.com/trust/security/products/commerce/apsb26-153.html			
CVE-2026-48382	10,0	Adobe Experience Manager	Incorrect Authorization	2026.9.28187 and earlier; 6.5 LTS SP3 and earlier; 6.5.25 and earlier	https://helpx.adobe.com/security/products/experience-manager/apsb26-152.html			
CVE-2026-89111	10,0	The SAP Cloud SDK for Python	Server-Side Request Forgery (SSRF)	sap-cloud-sdk < 0.45.2	https://github.com/SAP/cloud-sdk-python/security/advisories/GHSA-4mv3-jxxm-9cx2 https://url.sap/sapsecuritypatchday			
CVE-2026-89309	10,0	two distinct cases	Missing Authentication for Critical Function	prior to 2.0.7; prior to 2.1.2; prior to 2.2.1; 1.7.*, 1.8.*, 1.9.*, 1.10.*, 1.11.*	https://www.itl-software.com/de/cve-2026-89309-cve-2026-89310			
CVE-2026-94603	10,0	Podman	Protection Mechanism Failure	>= 4.4.0, < 5.8.8; >= 6.0.0, < 6.1.3	https://github.com/podman-container-tools/podman/commit/2470629 0d5c974f078d8ca284026802515f28e92 https://github.com/podman-container-tools/podman/commit/3721ff82ffb44a4ceeaecc5abd3808e924a6b669 https://github.com/podman-container-tools/podman/commit/450c64426dbcff1097d3c7911d791101e3d16f4c https://github.com/podman-container-tools/podman/commit/7728ba0a90094408ad9078e36c3622a651d49616 https://github.com/podman-container-tools/podman/commit/c74b1d37b3fb834b0de43e176565d9d8c254b627 https://github.com/podman-container-tools/podman/commit/ea9243e04d1db3886dc3a51ee3300ffb547cfc02	none	yes	total
CVE-2026-106042	9,9	Ivanti Xtraction	External Control of File Name or Path	before version 2026.4	https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Xtraction-Multiple-CVEs	none	no	total
CVE-2026-109412	9,9	Ivanti Neurons Patch for Intune	Exposed Dangerous Method or Function		https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Neurons-Patch-for-Intune-October-2026			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-77366	9,9	obsidian-tc	Authorization Bypass Through User-Controlled Key; Incorrect Authorization	Prior to 1.3.1	https://github.com/The-40-Thieves/obsidian-tc/commit/38b4992e87dc2715564236e1a42d005ab05a0194 https://github.com/The-40-Thieves/obsidian-tc/pull/72 https://github.com/The-40-Thieves/obsidian-tc/releases/tag/v1.3.1 https://github.com/The-40-Thieves/obsidian-tc/security/advisories/GHSA-84c9-qgpg-2pg5	none	no	total
CVE-2026-77459	9,9	Argo CD	Incorrect Authorization	>= 2.10.0, <= 2.14.21; >= 3.0.0, < 3.3.15; >= 3.4.0, < 3.4.10; >= 3.5.0, < 3.5.4; >= 3.6.0-rc1, < 3.6.0-rc2	https://github.com/argoproj/argo-cd/commit/1149cdc6e932208c4402183cc3d7b7485239940c https://github.com/argoproj/argo-cd/commit/4bc8085b0a6d2296b849539d3d09fc7be7a4a511 https://github.com/argoproj/argo-cd/commit/7f0a05834b05103d69d7c150e1ee36541b314696 https://github.com/argoproj/argo-cd/commit/d5dd7019ee65be8895133fe4df554e28074242c4 https://github.com/argoproj/argo-cd/releases/tag/v3.3.15 https://github.com/argoproj/argo-cd/releases/tag/v3.4.10			
CVE-2026-89107	9,9	SAP S/4HANA (Manage Substitution/Validation Rules)	Improper Control of Generation of Code ('Code Injection')	S4CORE 105; 106; 107; 108; 109	https://me.sap.com/notes/3805589 https://url.sap/sapsecuritypatchday	none	no	total
CVE-2026-89110	9,9	certain portal functionality	Exposed Dangerous Method or Function	VC70RUNTIME 7.50	https://me.sap.com/notes/3797111 https://url.sap/sapsecuritypatchday	none	no	total
CVE-2025-71429	9,8	GPT-SoVITS; tools/uvr5/vr	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	through 20250606v2pro	https://github.com/RVC-Boss/GPT-SoVITS https://github.com/RVC-Boss/GPT-SoVITS/blob/d7c2210da8c013e81a94bfc7b811a477c99fd506/tools/uvr5/vr.py#L143 https://github.com/RVC-Boss/GPT-SoVITS/issues/2319 https://www.vulncheck.com/advisories/gpt-sovits-through-20250606v2pro-os-command-injection-via-uvr5-vr-py	none	yes	total
CVE-2026-104252	9,8	Vitess	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Prior to 23.0.5 and 24.0.2	https://github.com/vitessio/vitess/commit/3140c1846cd120db34f33b2083139b4ab638aed2 https://github.com/vitessio/vitess/commit/976e1e0d78f9d29d02e5e31b4aa7e180648f08af https://github.com/vitessio/vitess/commit/c1ed96302e658190168c971afdac730cf70e43f7 https://github.com/vitessio/vitess/pull/20255 https://github.com/vitessio/vitess/pull/20273 https://github.com/vitessio/vitess/pull/20274			
CVE-2026-106173	9,8	Fortinet FortiSIEM	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	7.5.0; 7.4.0 through 7.4.2; 7.3.0 through 7.3.5; 7.2.0 through 7.2.7; 7.1.0 through 7.1.9; 7.0.0 through 7.0.4	https://fortiguard.fortinet.com/psirt/FG-IR-26-180	none	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-2026-108598	9,8	Floci	Improper Control of Generation of Code ('Code Injection')	before 2.2.0	https://github.com/floci-io/floci https://github.com/floci-io/floci/blob/560b3e4aae61cea3ac7d4d51843bdffd0e3085fd/src/main/java/io/github/hectorvent/floci/services/apigateway/VtlTemplateEngine.java#L74-L114 https://github.com/floci-io/floci/commit/144b90e6fa861a5ac882e99a090d503da01945c4 https://github.com/floci-io/floci/releases/tag/2.2.0 https://github.com/floci-io/floci/security/advisories/GHSA-3p4c-wp7w-mgjx https://github.com/ghostx-86/exploitarium/tree/main/floci-apigateway-vtl-rce-poc	poc	yes	total
CVE-2026-108707	9,8	Wukong_HRM through commit; ParamAspect that	Improper Authentication	186115e1a5a0b827ad9596ff8c2f3a876fb0cc55 and earlier	https://github.com/AnkesKasty/cve-request-poc/blob/a7b6d1423555812d8efa26c91c5d0683164b31e5/Wukong_HRM/poc_attachment_download_idor.py https://github.com/AnkesKasty/cve-request-poc/blob/a7b6d1423555812d8efa26c91c5d0683164b31e5/Wukong_HRM/poc_employee_export_pii.py https://github.com/AnkesKasty/cve-request-poc/blob/a7b6d1423555812d8efa26c91c5d0683164b31e5/Wukong_HRM/poc_salary_slip_detail_read.py https://github.com/WuKongOpenSource/Wukong_HRM/blob/186115e1a5a0b827ad9596ff8c2f3a876fb0cc55/common/common-web/src/main/java/com/kakarote/core/config/ParamAspect.java#L35-L55 https://github.com/WuKongOpenSource/Wukong_HRM/blob/186115e1a5a0b827ad9596ff8c2f3a876fb0cc55/hrm/hrm-web/src/main/java/com/kakarote/hrm/common/EmployeeAspect.java#L28-L45 https://www.vulncheck.com/advisories/wukong-hrm-through-commit-186115e-authentication-bypass-via-paramaspect			
CVE-2026-109566	9,8	Rapyd Admin	Use of Hard-coded Credentials	before 9.20.0	https://github.com/zofe/rapyd-admin https://github.com/zofe/rapyd-admin/blob/v9.19.0/src/Modules/Auth/Database/Seeders/AuthSeeder.php#L29-L34 https://github.com/zofe/rapyd-admin/commit/acd6ee85f9e5ccec67199673b039c605d161406a https://github.com/zofe/rapyd-admin/releases/tag/v9.20.0 https://www.vulncheck.com/advisories/rapyd-admin-9.0.0-before-9.20.0-hard-coded-super-admin-credentials-via-authseeder			
CVE-2026-53709	9,8	MCP Context Forge	Improper Authentication; Use of Hard-coded Cryptographic Key; Use of Hard-coded Credentials; Initialization of a Resource with an Insecure Default	Prior to 1.0.2	https://github.com/IBM/mcp-context-forge/commit/2af690f894b6e35f5f21190fdab1505f023a5272 https://github.com/IBM/mcp-context-forge/releases/tag/v1.0.2 https://github.com/IBM/mcp-context-forge/security/advisories/GHSA-m8rv-5m6m-32ff			
CVE-2026-63146	9,8	Omnispace Agora Project	Improper Control of Generation of Code ('Code Injection')	before 26.10.0	https://github.com/xech/agora-project/releases/tag/26.10 https://www.agora-project.net/ https://www.vulncheck.com/advisories/omnispace-agora-project-php-code-injection-via-config-inc-php			
CVE-2026-69227	9,8	Portal for ArcGIS	Missing Authentication for Critical Function	12.2 and earlier	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/september-2026-arcgis-security-bulletin	none	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-2026-87689	9,8	The Metasploit Framework Web Service REST API (msf-ws)	Missing Authentication for Critical Function	through 6.5.4	https://github.com/rapid7/metasploit-framework https://github.com/rapid7/metasploit-framework/releases/tag/6.5.5	none	yes	total
CVE-2026-102238	9,6	Visual Studio Code	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	1.0.0 prior to 1.141.1	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-102238	none	no	total
CVE-2026-108261	9,3	Tina	Origin Validation Error; Unintended Proxy or Intermediary ('Confused Deputy'); URL Redirection to Untrusted Site ('Open Redirect')	< 3.14.0; < 2.5.14	https://github.com/tinacms/tinacms/commit/b57dbf4b56201aef15cd92caa49fd12ab96bbecf https://github.com/tinacms/tinacms/pull/7522 https://github.com/tinacms/tinacms/releases/tag/@tinacms/app@2.5.14 https://github.com/tinacms/tinacms/releases/tag/tinacms@3.14.0 https://github.com/tinacms/tinacms/security/advisories/GHSA-x34j-47hf-4xg7	poc	no	total
CVE-2026-110116	9,1	Digital-Infrastructure	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	9.6.5 through 9.6.11	https://github.com/risesoft-y9/Digital-Infrastructure/blob/v9.6.11/y9-digitalbase-module/y9-module-filemanager/risenet-y9boot-webapp-filemanager/src/main/java/net/risesoft/y9public/controller/Y9FileController.java#L168-L182 https://hackmd.io/@1ExmmukzRMWN7B4qO4W-4Q/digital-infrastructure-filemanager-path-traversal-rw https://www.vulncheck.com/advisories/digital-infrastructure-9.6.5-through-9.6.11-path-traversal-via-filemanager-storefile	none	yes	partial
CVE-2026-52394	9,1	DeepSeek	Insertion of Sensitive Information Into Sent Data; Generation of Error Message Containing Sensitive Information		http://deepseek.com https://gist.github.com/CAP-TAIN1275/48a0b7d67d0e58cb05c607e0d715447c	poc	yes	total
CVE-2026-89108	9,1	SAP Manufacturing Integration and Intelligence (Configuration Service)	Missing Authorization	XMII 15.4; 15.5	https://me.sap.com/notes/3798788 https://url.sap/sapsecuritypatchday	none	no	total
CVE-2025-46773	8,8	FortiAnalyzer Cloud; FortiAnalyzer	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7.6.0 through 7.6.4; 7.4.0 through 7.4.7; 7.6.2 through 7.6.4; 7.4.1 through 7.4.7; 7.2.1 through 7.2.11	https://fortiguard.fortinet.com/psirt/FG-IR-25-246	none	no	total
CVE-2025-57739	8,8	FortiMail	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7.6.0 through 7.6.3; 7.4.0 through 7.4.5; 7.2.0 through 7.2.8	https://fortiguard.fortinet.com/psirt/FG-IR-26-184	none	no	total
CVE-2026-102855	8,8	Microsoft Office Visio	Heap-based Buffer Overflow	16.0.1 prior to https://aka.ms/OfficeSecurityReleases; 16.0.1 prior to 16.0.14334.20974; 16.0.0 prior to 16.0.17932.21056	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-102855	none	no	total
CVE-2026-104085	8,8	odt2spip plugin for SPIP	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	before 4.4.0	https://plugins.spip.net/odt2spip.html https://www.vulncheck.com/advisories/odt2spip-os-command-injection-via-document-filename	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-2026-108375	8,8	dataclasses-avroschema	Improper Control of Generation of Code ('Code Injection')	From version 0.38.0 through 0.70.5	https://github.com/marcosschroh/dataclasses-avroschema/commit/01e6d5e15ab0ff69faac39a340d21b85da1e852f https://github.com/marcosschroh/dataclasses-avroschema/releases/tag/0.70.6 https://github.com/marcosschroh/dataclasses-avroschema/security/advisories/GHSA-9h8h-264x-jcq2	poc	no	total
CVE-2026-108550	8,8	SkillHub	Incorrect Authorization	before 0.2.22	https://github.com/iflytek/skillhub https://github.com/iflytek/skillhub/blob/v0.2.21/server/skillhub-auth/src/main/java/com/iflytek/skillhub/auth/merge/AccountMergeService.java#L95-L109 https://github.com/iflytek/skillhub/commit/45228996c7dd67f9304dba5b221fef15138a7fc4 https://github.com/iflytek/skillhub/issues/921 https://github.com/iflytek/skillhub/releases/tag/v0.2.22 https://www.vulncheck.com/advisories/skillhub-before-0.2.22-account-takeover-via-account-merge-flow			
CVE-2026-109305	8,8	Craft CMS	Improper Neutralization of Special Elements Used in a Template Engine	before 5.10.14	https://github.com/craftcms/cms/security/advisories/GHSA-vfcw-xv8p-8rj2 https://www.vulncheck.com/advisories/craft-cms-5.10.2-before-5.10.14-twig-sandbox-bypass-rce-via-has-some-has-every	none	no	total
CVE-2026-109308	8,8	cms	Improper Control of Generation of Code ('Code Injection')	before 4.18.7 and 5.0.0; before 5.10.14	https://github.com/craftcms/cms/security/advisories/GHSA-5m2g-hhqr-84pc https://www.vulncheck.com/advisories/craft-cms-4.0.0-before-4.18.7-and-5.0.0-before-5.10.14-rce-via-actioncacheupdates-behavior-injection	none	no	total
CVE-2026-109318	8,8	Grav Git Sync	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	1.0.2 through 3.4.12	https://github.com/getgrav/grav/security/advisories/GHSA-c89w-55m3-fmf7 https://www.vulncheck.com/advisories/grav-git-sync-1.0.2-through-3.4.12-command-injection-via-commit-author	none	no	total
CVE-2026-109569	8,8	sandboxed.sh	Initialization of a Resource with an Insecure Default	through 1.3.0	https://github.com/Th0rgal/orb https://github.com/Th0rgal/orb/commit/4ab42e91b16c452f77d93ca69a040a54229b0aa2 https://www.vulncheck.com/advisories/sandboxed-sh-through-1.3.0-container-escape-via-nsenter-missing-root-namespace	none	no	total
CVE-2026-109676	8,8	FreeRDP	Use After Free	before 3.32.0	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-369h-7h2p-4685 https://www.vulncheck.com/advisories/freerdp-3.0.0-beta1-before-3.32.0-use-after-free-via-smartcard-connect			
CVE-2026-11731	8,8	the listed NETGEAR RAX series models	Authentication Bypass Using an Alternate Path or Channel	prior to v1.0.15.110	https://www.netgear.com/support/product/rax30	none	no	total
CVE-2026-11732	8,8	the website blocking feature (Block Sites) of the listed NETGEAR router models	Improper Input Validation	prior to V2.3.4.12; prior to V1.0.14.108; prior to V1.0.5.34; prior to V1.0.10.72	https://www.netgear.com/support/product/cax30/ https://www.netgear.com/support/product/rax30/ https://www.netgear.com/support/product/rax5/ https://www.netgear.com/support/product/raxe300/	none	no	total
CVE-2026-59241	8,8	SIMATIC WinCC	Incorrect Privilege Assignment	V7; < V8	https://cert-portal.siemens.com/productcert/html/ssa-550198.html			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-87690	8,8	The Metasploit Framework post module post/apple_ios/gather/ios_image_gather	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	prior to 6.5.5	https://github.com/rapid7/metasploit-framework https://github.com/rapid7/metasploit-framework/pull/21880 https://github.com/rapid7/metasploit-framework/releases/tag/6.5.5 https://www.rapid7.com/blog/post/pt-metasploit-wrap-up-belgian-waffles-chocolates-and-modules-frites/	none	no	total
CVE-2026-89113	8,8	SAP Commerce Cloud (OOTB Code)	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	COM_CLOUD 2211-JDK21	https://me.sap.com/notes/3800517 https://url.sap/sapsecuritypatchday	none	no	total
CVE-2026-89196	8,8	RUGGEDCOM CROSSBOW (All	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	< V6.0)	https://cert-portal.siemens.com/productcert/html/ssa-508506.html			
CVE-2026-103845	8,6	Dimension; arbitrary code execution in the context of the current user	Uncontrolled Search Path Element	4.1.8 and earlier	https://www.adobe.com/trust/security/products/dimension/apsb26-171.html	none	no	total
CVE-2026-104935	8,6	ICS	Authentication Bypass by Spoofing	before version 25.1.3.0; version 22.7R2.14 or prior	https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-CVE-2026-104935	active	yes	total
CVE-2026-78557	8,3	Industrial Edge App Publisher (All	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	< V1.27.9)	https://cert-portal.siemens.com/productcert/html/ssa-968435.html	none	no	total
CVE-2020-37279	8,1	easy-pdf-merge	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	0.1.0 through 0.2.6	https://github.com/karuppiah7890/easy-pdf-merge https://github.com/karuppiah7890/easy-pdf-merge/blob/v0.2.6/source/lib/PDFMerger.js#L71-L75 https://github.com/karuppiah7890/easy-pdf-merge/pull/28 https://github.com/karuppiah7890/easy-pdf-merge/pull/45 https://www.vulncheck.com/advisories/easy-pdf-merge-0.1.0-through-0.2.6-os-command-injection-via-merge-function	poc	no	total
CVE-2026-109399	8,1	SWUpdate	Improper Certificate Validation	through 2026.05.1	https://github.com/sbabic/swupdate https://github.com/sbabic/swupdate/blob/2026.05.1/crypto/swupdate_cms_verify_openssl.c https://github.com/sbabic/swupdate/commit/e66c5640664a31668926a24c0c84b6b6570dc0d9 https://groups.google.com/g/swupdate/c/dsoMcGFnEns https://www.vulncheck.com/advisories/swupdate-through-2026.05.1-cms-signature-verification-bypass-via-embedded-intermediates			
CVE-2026-109422	8,1	NetEase Cloud Music for Windows	Exposed Dangerous Method or Function	3.1.38; 3.1.39.205426	https://gist.github.com/LeoWSY-hashblue/10e5383fc2d4d75faf74a9507c6bba9f https://hr.163.com/product.html/music https://www.vulncheck.com/advisories/netease-cloud-music-rce-via-os-navigateexternal-ipc			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-110097	8,1	Ikaros	Improper Authentication	1.2.0 through 1.2.5	https://github.com/ikaros-dev/ikaros/blob/v1.2.5/server/src/main/java/run/ikaros/server/security/SecurityEndpoint.java#L80-L118 https://github.com/ikaros-dev/ikaros/blob/v1.2.5/server/src/main/java/run/ikaros/server/security/authentication/jwt/JwtAuthenticationFilter.java#L30-L46 https://github.com/ikaros-dev/ikaros/blob/v1.2.5/server/src/main/java/run/ikaros/server/security/authentication/jwt/JwtAuthenticationProvider.java#L57-L112 https://github.com/ikaros-dev/ikaros/releases/tag/v1.2.5 https://hackmd.io/@1ExmmukzRMWN7B4gQ4W-4Q/ikaros-2fa-bypass-temp-token https://www.vulncheck.com/advisories/ikaros-1.2.0-through-1.2.5-totp-authentication-bypass-via-temp-token			
CVE-2026-110108	8,1	MateCloud	Missing Authorization	through 5.0.8	https://github.com/mateaix/matecloud https://github.com/mateaix/matecloud/blob/57b1edc0f0b8b964448e2d41ef7ba98751e71d8d/mate-biz/mate-system/src/main/java/vip/mate/system/admin/trigger/controller/StorageController.java#L45-L118 https://github.com/mateaix/matecloud/blob/57b1edc0f0b8b964448e2d41ef7ba98751e71d8d/mate-gateway/src/main/resources/application.yml#L80-L85 https://hackmd.io/@1ExmmukzRMWN7B4gQ4W-4Q/matecloud-storage-admin-missing-authz https://www.vulncheck.com/advisories/matecloud-through-5.0.8-missing-authorization-via-api-v1-admin-storage-api			
CVE-2026-110124	8,1	FastBee	Authorization Bypass Through User-Controlled Key	through 2.1.0	https://github.com/kerwincui/FastBee/blob/v1.2.1/springboot/wumei-iot/src/main/java/com/ruoyi/iot/controller/DeviceController.java#L118-L213 https://github.com/kerwincui/FastBee/blob/v2.1.0/springboot/fastbee-open-api/src/main/java/com/fastbee/data/controller/DeviceController.java#L119-L211 https://github.com/kerwincui/FastBee/blob/v2.1.0/springboot/fastbee-service/fastbee-iot-service/src/main/java/com/fastbee/iot/service/impl/DeviceServiceImpl.java#L105-L125 https://hackmd.io/@1ExmmukzRMWN7B4gQ4W-4Q/fastbee-device-ownership-idor https://www.vulncheck.com/advisories/fastbee-through-2.1.0-idor-via-devicecontroller-iot-device-endpoints			
CVE-2026-57458	8,1	Vikunja	Improper Privilege Management	= 2.3.0	https://github.com/go-vikunja/vikunja/commit/4ae2e093014881052ed8f8ecd8bcb9adf83dd276 https://github.com/go-vikunja/vikunja/releases/tag/v2.4.0 https://github.com/go-vikunja/vikunja/security/advisories/GHSA-v3p6-34mc-hj7v	poc	no	total
CVE-2026-103840	7,8	Substance3D - Stager	Out-of-bounds Read	3.1.8 and earlier	https://www.adobe.com/trust/security/products/substance3d-stager/apsb26-170.html			
CVE-2026-108094	7,8	A	Use After Free		https://access.redhat.com/security/cve/CVE-2026-108094 https://bugzilla.redhat.com/show_bug.cgi?id=2549511	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-2026-108953	7,8	mac-shell-mcp	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	before 2.0.0	https://github.com/cfdude/mac-shell-mcp https://github.com/cfdude/mac-shell-mcp/blob/1c1708201abb7a18c83075e1bf933e7a92cbeb9f/src/services/command-service.ts#L257-L340 https://github.com/cfdude/mac-shell-mcp/commit/932ce733cde07bb30b1f186303e6692dbb5d087a https://github.com/cfdude/mac-shell-mcp/issues/45 https://www.vulncheck.com/advisories/mac-shell-mcp-before-2.0.0-os-command-injection-via-execute-command-arguments	none	no	total
CVE-2026-108976	7,8	GNU Emacs	Incomplete List of Disallowed Inputs	before 31.2; through 2.8.2)	https://ftp.gnu.org/gnu/tramp/tramp-2.8.2.tar.gz https://www.openwall.com/lists/oss-security/2026/08/21/1 https://www.openwall.com/lists/oss-security/2026/10/11/1			
CVE-2026-109358	7,8	Edgeless Systems Contrast	Incorrect Permission Assignment for Critical Resource	before 1.24.1	https://github.com/edgelesssys/contrast/security/advisories/GHSA-376m-h37w-4rvq https://www.vulncheck.com/advisories/edgeless-systems-contrast-1.8.0-before-1.24.1-world-writable-containerd-config-privilege-escalation	none	no	total
CVE-2026-35001	7,8	OpenS100 through commit daa35b; the S-102 Bathymetric Surface parser that	Heap-based Buffer Overflow; Integer Overflow or Wraparound	daaa35b19b789aa4b170bdcc300763a287d73164 and earlier	https://doi.org/10.3390/s26206448 https://www.vulncheck.com/advisories/opens100-s-102-parser-integer-overflow-heap-buffer-overflow			
CVE-2026-95837	7,8	containerd	Improper Privilege Management	>= 2.1.0, < 2.2.7; >= 2.3.0, < 2.3.4	https://github.com/containerd/containerd/commit/928c03c6898cad95f795300281fdff0dbc55a32f https://github.com/containerd/containerd/pull/13913 https://github.com/containerd/containerd/security/advisories/GHSA-p7v4-vr35-mj6f	none	no	total
CVE-2026-106047	7,7	the template export functionality of Ivanti Xtraction	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	before version 2026.4	https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Xtraction-Multiple-CVEs	none	no	partial
CVE-2026-109359	7,7	Contrast	Insufficient Verification of Data Authenticity	before 1.24.1	https://github.com/edgelesssys/contrast/security/advisories/GHSA-rxcv-p3px-m3c3 https://www.vulncheck.com/advisories/contrast-1.8.0-before-1.24.1-mesh-ca-key-cross-manifest-exposure-via-peer-recovery	none	no	partial
CVE-2026-61642	7,7	Squid	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')	before 7.6	https://github.com/squid-cache/squid/commit/d06f48de8b8cc9a378cb91ecfe8e89b6e81696d2 https://github.com/squid-cache/squid/commit/d808a7c825a70275113790471135c9c4d547ee51 https://github.com/squid-cache/squid/pull/2427 https://github.com/squid-cache/squid/pull/2431 https://github.com/squid-cache/squid/releases/tag/SQUID_7_6 https://github.com/squid-cache/squid/security/advisories/GHSA-537g-4gfh-w7m6	none	no	partial
CVE-2026-72895	7,7	SIMATIC IPC BX-21A (All	Use of Default Cryptographic Key	< V31.01.13); < V1.1.4); < V28.01.15)	https://cert-portal.siemens.com/productcert/html/ssa-159454.html			
CVE-2026-75888	7,7	the OpenShift console	Server-Side Request Forgery (SSRF)		https://access.redhat.com/security/cve/CVE-2026-75888 https://bugzilla.redhat.com/show_bug.cgi?id=2517888			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-82416	7,7	FrankenPHP	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition'); Exposure of Data Element to Wrong Session	Prior to 1.12.5	https://github.com/php/frankenphp/commit/be24d82531675f90862b8cde1e9fc7e9ee855aa5 https://github.com/php/frankenphp/pull/2523 https://github.com/php/frankenphp/releases/tag/caddy/v1.12.5 https://github.com/php/frankenphp/security/advisories/GHSA-v3ph-cqgh-r8p5	none	no	total
CVE-2026-54640	7,6	OpenRemote	Improper Restriction of XML External Entity Reference	Prior to 1.24.2	https://github.com/openremote/core/commit/c28d3c60ebc2da68d9b6c4a6d7a5ad875a255ee9 https://github.com/openremote/core/releases/tag/1.24.2 https://github.com/openremote/core/security/advisories/GHSA-7v6w-c3f4-9wpq	none	no	partial
CVE-2026-103030	7,5	Dio	Exposure of Sensitive Information to an Unauthorized Actor	>= 1.0.0, < 2.8.0	https://github.com/cfug/dio/commit/9d7ac913340084f3b4987b121e076f28d637a81e https://github.com/cfug/dio/releases/tag/http2_adapter_v2.8.0 https://github.com/cfug/dio/security/advisories/GHSA-cr65-55v9-xhvv	poc	yes	partial
CVE-2026-103902	7,5	DigiDoc libdigidocpp, DigiDoc DigiDoc4, DigiDoc DigiDoc Android, and DigiDoc DigiDoc iOS	Improper Verification of Cryptographic Signature	4.0; before 4.5.0; before 4.11.0; before 3.1.0; before 3.1.0.	https://github.com/open-eid/libdigidocpp/pull/735 https://www.id.ee/en/article/id-tarkvara-uus-versioon-267-on-avalikustatud/			
CVE-2026-108553	7,5	OpenRefine	Cross-Site Request Forgery (CSRF)	through 3.10.1	https://github.com/OpenRefine/OpenRefine https://github.com/OpenRefine/OpenRefine/blob/bde8a36dc188f7846aeafc2910969e7d0fbc8e7c/extensions/jython/src/com/google/refine/jython/JythonEvaluable.java#L142 https://github.com/OpenRefine/OpenRefine/blob/bde8a36dc188f7846aeafc2910969e7d0fbc8e7c/main/src/com/google/refine/commands/row/GetRowsCommand.java#L174-L186 https://github.com/OpenRefine/OpenRefine/blob/bde8a36dc188f7846aeafc2910969e7d0fbc8e7c/modules/core/src/main/java/com/google/refine/browsing/facets/ListFacet.java#L327-L339 https://github.com/OpenRefine/OpenRefine/issues/7999 https://www.vulncheck.com/advisories/openrefine-through-3.10.1-csrf-to-rce-via-get-rows-command			
CVE-2026-109560	7,5	Continue CLI (@continuedev/cli)	Incorrect Authorization	through 1.5.47	https://github.com/continuedev/continue https://github.com/continuedev/continue/blob/d3f60ba9dd3fb5bfd3c91d6fbb41ce1aa768db45/extensions/cli/src/permissions/permissionChecker.ts#L162-L174 https://github.com/continuedev/continue/blob/d3f60ba9dd3fb5bfd3c91d6fbb41ce1aa768db45/extensions/cli/src/permissions/policyWriter.ts#L18-L31 https://github.com/continuedev/continue/issues/13288 https://www.vulncheck.com/advisories/continue-cli-through-1.5.47-bash-permission-rule-bypass-via-command-chaining	poc	no	total
CVE-2026-109563	7,5	N3.js	Inefficient Regular Expression Complexity	before 2.11.1	https://github.com/rdfjs/N3.js https://github.com/rdfjs/N3.js/commit/b1c497fddb02c4772d61916bd2634115f45f424d https://github.com/rdfjs/N3.js/pull/760 https://www.vulncheck.com/advisories/n3-js-before-2.11.1-redos-via-n3lexer-numeric-literal-regex			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-109832	7,5	gnome-remote-desktop as shipped in Red Hat Enterprise Linux	Loop with Unreachable Exit Condition ('Infinite Loop')		https://access.redhat.com/security/cve/CVE-2026-109832 https://bugzilla.redhat.com/show_bug.cgi?id=2550352	none	yes	partial
CVE-2026-109967	7,5	yt-dlp-web-ui	NULL Pointer Dereference	through 4.0.0	https://github.com/marcopiovanello/yt-dlp-web-ui https://github.com/marcopiovanello/yt-dlp-web-ui/blob/v4.0.0/server/formats/parser.go https://github.com/marcopiovanello/yt-dlp-web-ui/blob/v4.0.0/server/rpc/service.go https://github.com/vazzzy071-crypto/security-advisories/blob/main/advisories/2026-10-marcopiovanello-yt-dlp-web-ui-rpc-arg-injection.md https://www.vulncheck.com/advisories/yt-dlp-web-ui-through-4.0.0-null-pointer-dereference-dos-via-service-formats			
CVE-2026-110115	7,5	Risesoft Digital-Infrastructure	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	9.6.5 through 9.6.11	https://github.com/risesoft-y9/Digital-Infrastructure/blob/v9.6.11/y9-digitalbase-module/y9-module-filemanager/risenet-y9boot-webapp-filemanager/src/main/java/net/risesoft/y9public/controller/Y9FileController.java#L136-L166 https://hackmd.io/@1ExmmukzRMWN7B4gQ4W-4Q/digital-infrastructure-filemanager-path-traversal-rw https://www.vulncheck.com/advisories/digital-infrastructure-9.6.5-through-9.6.11-path-traversal-via-filemanager-retrievefilestream			
CVE-2026-110128	7,5	fuint through commit	Missing Authentication for Critical Function	4c4bc8a68e0a93d37c37ab374f72d64728c9e5f8 and earlier	https://github.com/fushengqian/fuint/blob/4c4bc8a68e0a93d37c37ab374f72d64728c9e5f8/fuint-application/src/main/java/com/fuint/common/config/WebConfig.java#L80-L101 https://github.com/fushengqian/fuint/blob/4c4bc8a68e0a93d37c37ab374f72d64728c9e5f8/fuint-application/src/main/java/com/fuint/module/clientApi/controller/ClientOrderController.java#L77-L80 https://hackmd.io/@1ExmmukzRMWN7B4gQ4W-4Q/fuint-order-detail-unauthenticated-idor https://www.vulncheck.com/advisories/fuint-through-commit-4c4bc8a-missing-authentication-via-clientapi-order-detail			
CVE-2026-58249	7,5	specially crafted requests handled by an internal protocol component	Integer Underflow (Wrap or Wraparound)	HDB 2.00; KRNL64UC 7.53; WEBDISP 7.53; 7.54; 7.77; 7.93; 9.16; XS_ADVANCED_RUNTIME 1.00; SAP_EXTENDED_APP_SERVICES 1; CONTSERV 7.53; KERNEL 7.53; 9.18; 9.19; 9.20	https://me.sap.com/notes/3765424 https://url.sap/sapsecuritypatchday	none	yes	partial
CVE-2026-85114	7,5	.NET Client Library for SIMATIC S7 Webserver API	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	< V3.3.61)	https://cert-portal.siemens.com/productcert/html/ssa-390352.html			
CVE-2026-95114	7,5	libwebsockets; the LEJP incremental parser in lib/misc/lejp	Out-of-bounds Read		https://gist.github.com/1820893135-pixel/34d3bc35f74eb0807e73b1df3f15af42 https://github.com/warmcat/libwebsockets/commit/736a4a26fce344766bc6618df87bf32193829dd0 https://github.com/warmcat/libwebsockets/commit/c404a205a98323a7f60e69fae532c5d26bf4a62a https://github.com/warmcat/libwebsockets/issues/3664	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-2026-102234	7,4	a security decision in Visual Studio Code	Reliance on Untrusted Inputs in a Security Decision	1.0.0 prior to 1.141.1	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-102234	none	no	partial
CVE-2026-53997	7,4	Portal del Hermano (portaldelher-mano.es)	Improper Restriction of Ex-cessive Authentication At-tempts; Weak Password Re-covery Mechanism for For-gotten Password	before 2026-10-06	https://beafn28.es/articulos/cve-2026-53997 https://netherman.app/ https://www.vulncheck.com/advisories/netherman-portal-del-hermano-account-takeover-via-password-reset-oracle			
CVE-2026-108548	7,3	AstronRPA	Improper Authentication	through 1.1.6	https://github.com/iflytek/astron-rpa https://github.com/iflytek/astron-rpa/blob/v1.1.6/backend/ai-service/app/dependencies/__init__.py#L10-L24 https://github.com/iflytek/astron-rpa/blob/v1.1.6/docker/volumes/nginx/lua/auth_handler.lua#L21-L35 https://github.com/iflytek/astron-rpa/issues/886 https://www.vulncheck.com/advisories/astronrpa-through-1.1.6-authentication-bypass-via-arbitrary-bearer-token	none	yes	partial
CVE-2026-108695	7,1	MultiVendorX WordPress plugin	Incorrect Authorization	through 5.0.19	https://github.com/multivendorx/multivendorx https://github.com/multivendorx/multivendorx/blob/8a717799b02f698e4b2b61a282062a41fbe15183/plugins/multivendorx/classes/RestAPI/Controllers/Settings.php#L157-L172 https://github.com/multivendorx/multivendorx/blob/8a717799b02f698e4b2b61a282062a41fbe15183/plugins/multivendorx/classes/RestAPI/Controllers/Settings.php#L77-L80 https://github.com/multivendorx/multivendorx/issues/2375 https://wordpress.org/plugins/dc-woocommerce-multi-vendor/ https://www.vulncheck.com/advisories/multivendorx-through-5.0.19-incorrect-authorization-via-settings-rest-endpoint	poc	no	partial
CVE-2026-109164	7,1	TDuck survey form	Authorization Bypass Through User-Controlled Key	through 6.0	https://github.com/AnkesKasty/cve-request-poc/blob/a7b6d1423555812d8efa26c91c5d0683164b31e5/tduck/poc_form_data_delete_idor.py https://github.com/TDuckCloud/tduck-survey-form/blob/43ffa9c993e38936fc4de7d8e5aee82bbaa19502/tduck-api/src/main/java/com/tduck/cloud/api/web/controller/UserFormResultController.java#L182-L187 https://github.com/TDuckCloud/tduck-survey-form/blob/43ffa9c993e38936fc4de7d8e5aee82bbaa19502/tduck-form/src/main/java/com/tduck/cloud/form/service/impl/UserFormDataServiceImpl.java#L149-L154 https://www.vulncheck.com/advisories/tduck-survey-form-through-6.0-authorization-bypass-via-user-controlled-submission-ids-in-post-user-form-data-delete-formkey			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-110119	7,1	Yshopmall	Authorization Bypass Through User-Controlled Key	through 2.0.0	https://github.com/quchengwuyue/yshopmall/blob/d1b20a2d76dfd98985410116db3aca8aca193b26/yshop-mall-boot/yshop-app/src/main/java/co/yixiang/modules/user/rest/UserAddressController.java#L117-L153 https://github.com/quchengwuyue/yshopmall/blob/d1b20a2d76dfd98985410116db3aca8aca193b26/yshop-mall-boot/yshop-mall/src/main/java/co/yixiang/modules/user/service/impl/YxUserAddressServiceImpl.java#L75-L114 https://hackmd.io/@1ExmmukzRMWN7B4gQ4W-4Q/yshopmall-member-api-ownership-idor https://www.vulncheck.com/advisories/yshopmall-through-2.0.0-idor-via-member-address-api-in-useraddresscontroller			
CVE-2026-110123	7,1	Makunet maku-boot	Missing Authorization	4.3.0 through 5.0.0	https://github.com/makunet/maku-boot/blob/4cd202b037e2ac47e366d4b0691fb387c764d308/maku-boot-system/src/main/java/net/maku/system/controller/SysMailConfigController.java#L53-L59 https://github.com/makunet/maku-boot/blob/4cd202b037e2ac47e366d4b0691fb387c764d308/maku-boot-system/src/main/java/net/maku/system/controller/SysMailConfigController.java#L79-L84 https://github.com/makunet/maku-boot/blob/4cd202b037e2ac47e366d4b0691fb387c764d308/maku-boot-system/src/main/java/net/maku/system/controller/SysSmsConfigController.java#L53-L59 https://github.com/makunet/maku-boot/releases/tag/v5.0.0 https://hackmd.io/@1ExmmukzRMWN7B4gQ4W-4Q/maku-boot-mail-sms-config-bfla https://www.vulncheck.com/advisories/makunet-maku-boot-4.3.0-through-5.0.0-missing-authorization-via-mail-and-sms-config-endpoints			
CVE-2026-89120	7,1	SAP ABAP Platform reintroduces a previously fixed authorization weakness	Initialization of a Resource with an Insecure Default	KERNEL 7.93; 9.16	https://me.sap.com/notes/3626303 https://url.sap/sapsecuritypatchday	none	no	partial
CVE-2026-108693	7,0	ImageMagick on Windows	Uncontrolled Search Path Element	through 7.1.2-33	https://github.com/ImageMagick/ImageMagick https://github.com/ImageMagick/ImageMagick/blob/211e5b975a0019a88dcef5f84c1193f46738d815/MagickCore/nt-base.c#L1469-L1511 https://github.com/ImageMagick/ImageMagick/blob/211e5b975a0019a88dcef5f84c1193f46738d815/MagickCore/nt-base.c#L2829-L2832 https://github.com/ghostx-86/exploitarium/tree/main/imagemagick-gs-delegate-hijack-poc https://www.vulncheck.com/advisories/imagemagick-through-7.1.2-33-and-6.9.13-58-uncontrolled-search-path-via-ghostscript-delegate	poc	no	total

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 Urges Patching Newly Exploited Vulnerability in Ivanti Connect Secure | CISA	• CVE-2026-104935	https://cisa.gov/news-events/alerts/2026/10/13/cisa-urges-patching-newly-exploited-vulnerability-ivanti-connect-secure
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA	▪ CVE-2026-96951 Microsoft Windows Command Injection Vulnerability ▪ CVE-2026-104935 Ivanti Connect Secure Authentication Bypass by Spoofing Vulnerability	https://cisa.gov/news-events/alerts/2026/10/13/cisa-adds-two-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: Windows 11 24H2 Home and Pro reached end of support	https://bleepingcomputer.com/news/microsoft/microsoft-windows-11-24h2-home-and-pro-reached-end-of-support
UK Housing Ombudsman Service investigates 'security incident'	https://bleepingcomputer.com/news/security/uk-housing-ombudsman-service-investigates-security-incident
Windows 11 KB5127648 & KB5126653 cumulative updates released	https://bleepingcomputer.com/news/microsoft/windows-11-kb5127648-and-kb5126653-cumulative-updates-released
Attacker Chains Three Ivanti Connect Secure Zero-Days for Root Access, Only Two Patched So Far	https://thehackernews.com/2026/10/attacker-chains-three-ivanti-connect.html
Google Partially Reverses Chrome Bug Bounty Cuts	https://securityweek.com/google-partially-reverses-chrome-bug-bounty-cuts
TFG London cyberattack disrupts systems at Hobbs and Whistles retailers	https://bleepingcomputer.com/news/security/tfg-london-cyberattack-disrupts-systems-at-hobbs-and-whistles-retailers
Meta Says Hackers Took Code, Personal Data of 1,500 in GitHub Breach	https://securityweek.com/meta-says-hackers-took-code-personal-data-of-1500-in-github-breach
European Retail Firms Confirm Cyber Incidents	https://infosecurity-magazine.com/news/retail-firms-confirm-cyber
Defenders Reluctant to Deploy Agentic AI as a Cybersecurity Tool	https://infosecurity-magazine.com/news/defenders-skeptical-agentic-ai
Anthropic Warns AI Models Could Soon Self-Replicate on Smart TVs and IoT Devices Without a Data Center	https://cybersecuritynews.com/anthropic-ai-self-replication-iot
Small AI Models Could Soon Self-Replicate on IoT Devices, Anthropic Warns	https://securityweek.com/small-ai-models-may-soon-be-able-to-self-replicate-on-iot-devices-anthropic-warns
LG Smart TVs Vulnerable to Pre-Auth Root Takeover From Local Network	https://thehackernews.com/2026/10/lg-smart-tvs-vulnerable-to-pre-auth.html

Privacy Policy	https://cybersecuritynews.com/privacy-policy-2
Article Publication and Retention Policy	https://cybersecuritynews.com/terms-of-service
About Us	https://cybersecuritynews.com/about-us
UK Government Announces Sweeping New AI Security Plans	https://infosecurity-magazine.com/news/uk-government-sweeping-ai-security
Cyberattack Prompts Grocery Giant Ahold Delhaize to Disconnect Systems	https://securityweek.com/cyberattack-prompts-ahold-delhaize-to-disconnect-systems
Fifth of CISOs Take Time Off to Avoid Patch Tuesday	https://infosecurity-magazine.com/news/fifth-cisos-take-time-off-avoid
Massive DDoS Attack Disrupts Ubuntu's Canonical Websites and Security APIs	https://cybersecuritynews.com/ubuntu-websites-ddos-attack
Yandex Data Center Outage Disrupts Access to Cloud Files Following Drone Attack	https://cybersecuritynews.com/yandex-data-center-service-outage

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
iRhythm Data Breach Impacts at Least 360,000 People	https://securityweek.com/irhythm-data-breach-impacts-over-360000-people
Karaoke Giant Reveals Data Breach Impacting Eight Million	https://infosecurity-magazine.com/news/karaoke-giant-data-breach-eight
Admin Password "123456" Led to 8.8 Million Danish CPR Data Breach	https://cybersecuritynews.com/admin-password-danish-data-breach

Vulnerabilities / Flaws / Zero-day

Αναφέρονται τεχνικά ελαττώματα ή αδυναμίες που ενδέχεται να αξιοποιηθούν άμεσα από επιτιθέμενους — είτε επειδή είναι zero-day είτε γιατί η διόρθωσή τους καθυστερεί. Περιλαμβάνονται περιπτώσεις όπου δεν απαιτείται αλληλεπίδραση με τον χρήστη ή όπου παρακάμπτονται βασικά μέτρα ασφαλείας. Πολύ χρήσιμο για ομάδες που ασχολούνται με threat detection.

Σύντομη περιγραφή / Τίτλος	URL
Microsoft October 2026 Patch Tuesday fixes 1,411 flaws, 3 zero-days	https://bleepingcomputer.com/news/microsoft/microsoft-october-2026-patch-tuesday-fixes-1-411-flaws-3-zero-days
Ivanti Zero-Day Chain Gave Attackers Root Access to Fully Patched VPN	https://securityweek.com/ivanti-zero-day-chain-gave-attackers-root-access-to-fully-patched-vpn
Critical FortiSandbox GUI Vulnerability Allows Remote Attackers to Bypass Authentication	https://cybersecuritynews.com/fortisandbox-gui-vulnerability
SAP Discloses Critical CVSS 10 Flaw in Cloud SDK for Python Allowing OAuth2 Credential Theft	https://thehackernews.com/2026/10/sap-discloses-critical-cvss-10-flaw-in.html

GitHub Tightens npm Publishing After Flaw Left 1,500+ Packages Vulnerable to Hijacking	https://thehackernews.com/2026/10/github-tightens-npm-publishing-after.html
Ivanti Connect Secure 0-Day Vulnerability Actively Exploited in the Wild	https://cybersecuritynews.com/ivanti-connect-secure-zero-day
Ivanti warns of Connect Secure zero-day exploited in attacks	https://bleepingcomputer.com/news/security/ivanti-warns-of-connect-secure-zero-day-exploited-in-attacks
Docker Hub flaw let attackers impersonate users, tamper with images	https://bleepingcomputer.com/news/security/docker-hub-flaw-let-attackers-impersonate-users-tamper-with-images
SAP warns of maximum severity OAuth2 SSRF security flaw	https://bleepingcomputer.com/news/security/sap-warns-of-maximum-severity-oauth2-ssrf-security-flaw
Two Critical MarkLogic Flaws Could Give Delegated Managers Persistent Admin Control	https://thehackernews.com/2026/10/two-critical-marklogic-flaws-could-give.html
Max-Severity SSRF Flaw in SonicWall SMA Devices Under Attack	https://darkreading.com/vulnerabilities-threats/max-severity-ssrf-flaw-sonicwall-sma-devices-under-attack
Critical GitLab Vulnerability Enables Arbitrary Code Execution Attacks on Servers	https://cybersecuritynews.com/gitlab-vulnerability-code-execution
Bricksforge WordPress Plugin Vulnerability Exploited in the Wild	https://securityweek.com/bricksforge-wordpress-plugin-vulnerability-exploited-in-the-wild
GitLab warns of max severity code execution vulnerability	https://bleepingcomputer.com/news/security/gitlab-warns-of-max-severity-rce-flaw-in-regex-compiler-engine
Critical SonicWall SMA 1000 Flaw Targeted in 135 Exploitation Attempts After Patch	https://thehackernews.com/2026/10/critical-sonicwall-sma-1000-flaw.html
Attackers Exploit CVSS 10.0 Bricksforge WordPress Flaw Enabling Unauthenticated RCE	https://thehackernews.com/2026/10/attackers-exploit-cvss-100-bricksforge.html
Critical SonicWall Vulnerability Exploited Days After Disclosure	https://securityweek.com/critical-sonicwall-vulnerability-exploited-days-after-disclosure
Anthropic Cuts Live Internet Access for Internal AI Tests After Claude Exploits Injection Flaws	https://thehackernews.com/2026/10/anthropic-cuts-live-internet-access-for.html

Patches / Updates / Fixes

Εδώ θα βρείτε τις πιο πρόσφατες διορθώσεις και ενημερώσεις ασφαλείας από προμηθευτές λογισμικού και hardware. Το περιεχόμενο αφορά συγκεκριμένα bugs ή exploits που έχουν ήδη δημοσιοποιηθεί, μαζί με οδηγίες για το πώς να εφαρμοστούν τα patches.

Σύντομη περιγραφή / Τίτλος	URL
Microsoft releases Windows 10 KB5126657 extended security update	https://bleepingcomputer.com/news/microsoft/microsoft-releases-windows-10-kb5126657-extended-security-update
Microsoft Fixes 1,118 Vulnerabilities in October Patch Tuesday and Introduces New Risk Cohorts	https://cybersecuritynews.com/microsoft-october-patch-tuesday-2026
Docker Fixes Critical Two-Year-Old Hub Flaw That Let One User Push Images as Another	https://thehackernews.com/2026/10/docker-fixes-critical-two-year-old-hub.html
Adobe Patches 176 Vulnerabilities Across 11 Products	https://securityweek.com/adobe-patches-140-vulnerabilities-across-10-products
GitLab Patches CVSS 10.0 Flaw That Could Let Unauthenticated Users Run Server Code	https://thehackernews.com/2026/10/gitlab-patches-cvss-100-flaw-that-could.html

Potential threats / Threat intelligence

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

Σύντομη περιγραφή / Τίτλος	URL
Weekly Recap: Helpdesk 0-Days, Rogue Certs, ShinyHunters Arrest, AI-Fooling Malware and More	https://thehackernews.com/2026/10/weekly-recap-helpdesk-0-days-rogue.html
Luna Moth Leaks Shed Light on Ransomware Group's Inner Workings	https://infosecurity-magazine.com/news/luna-moth-leaks-ransomware-playbook
WhatsApp Attachment Deploys Malware That Gains SYSTEM Access on Windows	https://cybersecuritynews.com/whatsapp-attachment-deploys-malware
Old Palo Alto VPN Vulnerability Remains a Target for Ransomware Groups	https://infosecurity-magazine.com/news/palo-alto-vpn-vulnerability-target
Nippon Columbia malware incident exposes 8.6 million karaoke fan records	https://bleepingcomputer.com/news/security/nippon-columbia-malware-incident-exposes-86-million-karaoke-fan-records
Ransomware Actors Exploiting Palo Alto GlobalProtect Flaw for Stealthy VPN Access	https://cybersecuritynews.com/palo-alto-globalprotect-flaw-vpn-access

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 επαγ-γελματιών ασφάλειας.

Σύντομη περιγραφή / Τίτλος	URL
Threat Intelligence Guide for US SOC Teams and CISOs: How to Choose the Right Solution	https://cybersecuritynews.com/threat-intelligence-guide
Meta Zurp AI Toolkit Connects Burp Suite With AI Coding Agents for Bug Bounty Research	https://cybersecuritynews.com/meta-zurp-ai-toolkit

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 10/10/2026–13/10/2026, 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/