

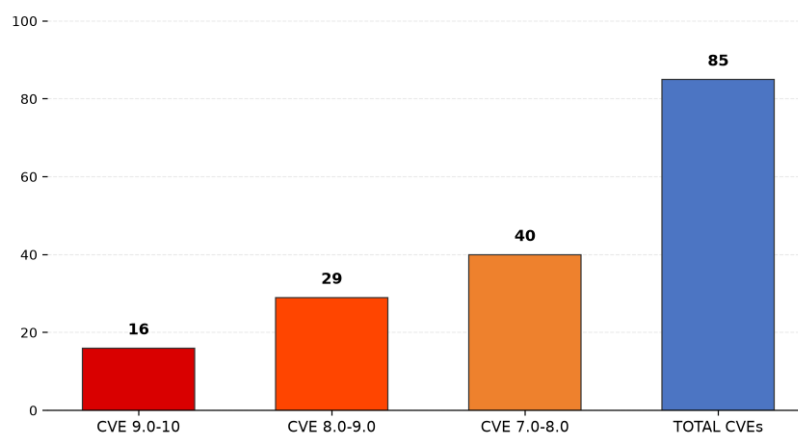


Newsletter on system vulnerabilities and cybersecurity news.

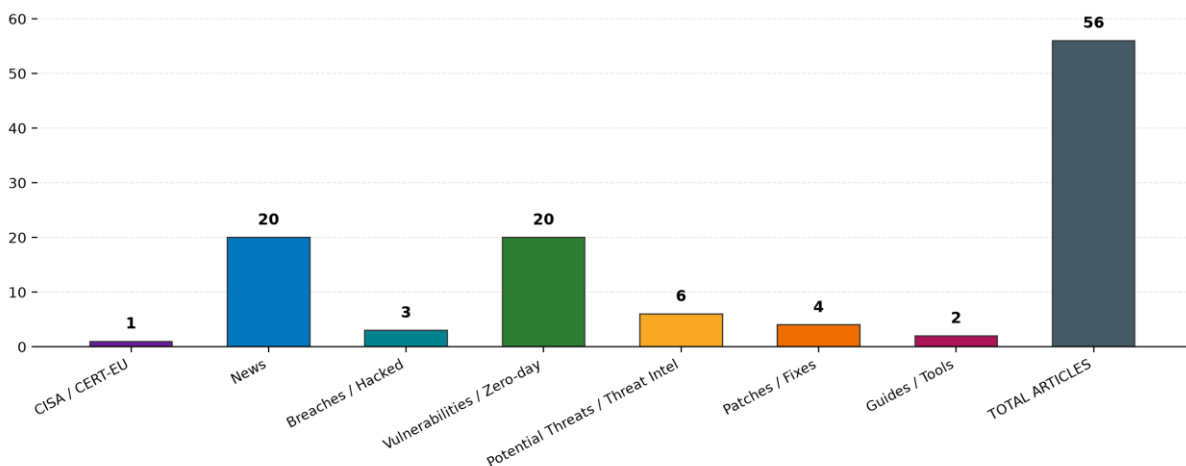
National Cyber Security Authority (NCSA)

Date: 12/09/2026 - 15/09/2026

of CVEs per CVSS score



of articles per section



Contents

Common Vulnerabilities and Exposures (CVEs)	3
CISA/CERT-EU Alerts & Advisories.....	14
News.....	15
Breaches / Compromised / Hacked.....	16
Vulnerabilities / Flaws / Zero-day.....	16
Patches / Updates / Fixes	17
Potential threats / Threat intelligence	17
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-2026-53710	10,0	MCP Context Forge	Improper Control of Generation of Code ('Code Injection'); Protection Mechanism Failure	Prior to 1.0.2	https://github.com/IBM/mcp-context-forge/commit/63a2900e6301b9c8a483a38d3737a1beb3a7ce89 https://github.com/IBM/mcp-context-forge/releases/tag/v1.0.2 https://github.com/IBM/mcp-context-forge/security/advisories/GHSA-xm98-3vcf-fph7	none	yes	total
CVE-2026-59971	10,0	MySQL MCP Server	Missing Authentication for Critical Function; Origin Validation Error	Prior to 0.4.2	https://github.com/designcomputer/mysql_mcp_server/commit/a96549f4a4d65443fd6e9c712324fba9a5c80a82 https://github.com/designcomputer/mysql_mcp_server/issues/92 https://github.com/designcomputer/mysql_mcp_server/releases/tag/v0.4.2 https://github.com/designcomputer/mysql_mcp_server/security/advisories/GHSA-rqfv-2mw9-78q2	none	no	total
CVE-2026-65381	10,0	macOS	Missing Authorization	versions from (including) 15.0 up to (excluding) 15.8; versions from (including) 26.0 up to (excluding) 26.7	https://support.apple.com/en-us/149035 https://support.apple.com/en-us/149042 https://support.apple.com/en-us/149043			
CVE-2026-85706	10,0	GitLab CE/EE affecting all	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18; before 19.1.8, 19.2; before 19.2.6; before 19.3.2	https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-85706	active	yes	total
CVE-2026-45579	9,9	DIRAC	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	>= 6r0, < 8.0.79; >= 9.0.0a1, < 9.0.22; >= 9.1.0, < 9.1.10	https://github.com/DIRACGrid/DIRAC/commit/8ec11072f48103d94e8b7cca831e2c7ce304d6c7 https://github.com/DIRACGrid/DIRAC/commit/99f1af88b525e69a77f204aebf7d8df3b6056142 https://github.com/DIRACGrid/DIRAC/commit/a6f75ce5d369254d46ca6f1d39e3f384366fa396 https://github.com/DIRACGrid/DIRAC/releases/tag/v8.0.79 https://github.com/DIRACGrid/DIRAC/releases/tag/v9.0.22 https://github.com/DIRACGrid/DIRAC/releases/tag/v9.1.10	none	no	total
CVE-2026-90937	9,9	froxlor versions	Improper Neutralization of CRLF Sequences ('CRLF Injection')	versions before 2.2.5	https://github.com/froxlor/froxlor/security/advisories/GHSA-c3p2-mi7v-5mrc https://www.vulncheck.com/advisories/froxlor-before-2.2.5-noinx-apache-configuration-injection-via-subdomain-redirect-url	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-2026-91998	9,9	Casdoor	Incorrect Authorization	through 4.4.0	https://github.com/casdoor/casdoor https://github.com/casdoor/casdoor/blob/v4.4.0/authz/authz.go#L174-L176 https://github.com/casdoor/casdoor/blob/v4.4.0/mcpsel/user.go https://github.com/casdoor/casdoor/blob/v4.4.0/routers/base.go#L122-L154 https://github.com/geo-chen/oss/blob/main/casdoor.md#finding-2-application-credential-authorization-bypass-in-apimcp-enables-unrestricted-cross-organization-user-administration https://www.vulncheck.com/advisories/casdoor-through-4.4.0-cross-organization-user-administration-via-api-mcp			
CVE-2023-54398	9,8	Yonyou U8 Cloud; the nc	Deserialization of Untrusted Data	1.0; 2.0; 2.1; 2.3; 2.5; 2.6; 2.65; 2.7; 3.0; 3.1; 3.2; 3.5; 3.6; 3.6sp	https://avd.alivun.com/detail?id=AVD-2023-1686894 https://blog.csdn.net/qq_41904294/article/details/134277353 https://cn-sec.com/archives/2182384.html https://security.yonyou.com/#/noticeInfo?id=400 https://www.vulncheck.com/advisories/yonyou-u8-cloud-java-deserialization-rce-via-filemanageservlet https://www.yonyou.com/Global/	poc	yes	total
CVE-2024-58385	9,8	Yonyou U8 CRM; the fillbacksettingedit	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18; 16.5; 16.1; 16.0; 15.1; 13	https://cn-sec.com/archives/3234745.html https://security.yonyou.com/#/noticeInfo?id=618 https://www.vulncheck.com/advisories/yonyou-u8-crm-sql-injection-via-fillbacksettingedit-php https://www.yonyou.com/Global/			
CVE-2026-62379	9,8	Open Access Management (OpenAM)	Improper Control of Generation of Code ('Code Injection'); Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	Prior to 16.1.2	https://github.com/OpenIdentityPlatform/OpenAM/commit/edcf968cad91a78b932dba4ad559ef94cbf35f5a https://github.com/OpenIdentityPlatform/OpenAM/releases/tag/16.1.2 https://github.com/OpenIdentityPlatform/OpenAM/security/advisories/GHSA-wq5r-wc3x-39vc	none	yes	total
CVE-2026-76461	9,8	the email parsing of Cisco AsyncOS Software for Cisco Secure Email Gateway	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	versions up to (excluding) 15.5.5-014; versions from (including) 16.0 up to (excluding) 16.0.4-302; versions from (including) 16.5 up to (excluding) 16.5.0-780	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-inj-2bLVGmhX	active	yes	total
CVE-2026-89026	9,8	The Issabel Framework, the web framework supporting Issabel PBX software, before commit b97dbaf	Use of Hard-coded Cryptographic Key	prior to b97dbaf0b71c1c36f841e672b664afbeb02773bd	https://github.com/IssabelFoundation/framework/commit/b97dbaf0b71c1c36f841e672b664afbeb02773bd https://www.vulncheck.com/advisories/issabel-pbx-hard-coded-jwt-key-rce-via-pbxapi-manager-originate			
CVE-2026-89040	9,8	Cluster (MSEC)	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')		https://github.com/Tencent/MSEC https://raw.githubusercontent.com/cisaqov/CSAF/develop/csaf_files/IT/white/2026/va-26-258-02.json https://www.cve.org/CVERecord?id=CVE-2026-89040			
CVE-2026-50006	9,1	Anyquery	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'); External Control of File Name or Path; Improper Access Control; Unrestricted Upload of File with Dangerous Type; Missing Authorization	Prior to 0.4.5	https://github.com/julien040/anyquery/commit/27f84fc168310455eaf81ec4ba87eed20298670c https://github.com/julien040/anyquery/releases/tag/0.4.5 https://github.com/julien040/anyquery/security/advisories/GHSA-xrcf-6jh3-qgvx	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-2026-53713	9,1	Envoy Gateway	Improper Input Validation	Prior to 1.7.4 and 1.8.1	https://github.com/envoyproxy/gateway/commit/5a78db82b7cf41c5bebbda2c50952892038a464 https://github.com/envoyproxy/gateway/commit/96e2b750868a459ace4b8b68e6a6e4fb0152b9b7 https://github.com/envoyproxy/gateway/commit/b4737180c7e597490c6363075c565fa8cf24eead https://github.com/envoyproxy/gateway/pull/9171 https://github.com/envoyproxy/gateway/pull/9172 https://github.com/envoyproxy/gateway/pull/9173	none	no	partial
CVE-2026-91995	9,1	pig	Unverified Password Change	before 4.1.0	https://github.com/geo-chen/oss/blob/main/pig.md https://github.com/pig-mesh/pig https://github.com/pig-mesh/pig/blob/v4.0.0/pig-upms/pig-upms-biz/src/main/java/com/pig4cloud/pig/admin/controller/SysRegisterController.java#L21-L53 https://github.com/pig-mesh/pig/blob/v4.0.0/pig-upms/pig-upms-biz/src/main/java/com/pig4cloud/pig/admin/service/impl/SysUserServiceImpl.java#L650-L669 https://github.com/pig-mesh/pig/commit/ce958668f399110b97b3f1fcc5f517ff9bafd535 https://github.com/pig-mesh/pig/issues/1249			
CVE-2023-46273	8,8	Extreme Networks IQ Engine	Stack-based Buffer Overflow	before 10.6r1a; through 10.6r4; before 10.6r5	https://extreme-networks.my.site.com/ExtraArticleDetail?an=000115356 https://extremenetworks.com	none	no	total
CVE-2023-50461	8,8	the direct_mail (aka Direct Mail) extension	Incorrect Authorization	through 9.5.1; 10.4 and above; 9.5 and below	https://typo3.org/security/advisory/typo3-ext-sa-2023-011	none	no	total
CVE-2026-16140	8,8	OpenBMC's IPMI implementation, phosphor-net-ipmid	Incorrect Authorization	ba6efc502e6b1fab8ed1ca677ae5eedd64b6361 and earlier	https://www.runzero.com/advisories/openbmc-ipmi-privsec-rakp-cve-2026-16140/ https://www.runzero.com/blog/lights-out-exposed/	none	no	total
CVE-2026-40058	8,8	the Falcon sensor for Windows	Time-of-check Time-of-use (TOCTOU) Race Condition	7.34 and above	https://www.crowdstrike.com/en-us/security-advisories/cve-2026-40058/	none	no	total
CVE-2026-52484	8,8	MitraStar GPT-2742GX4X5v6-SV GL_g2	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')		https://github.com/FelpM/Mitrastar_GPT-2742GX4X5v6-SV_GL_g2.5_100XNT0b23_3	poc	no	total
CVE-2026-58704	8,8	In Cellular Modem, there; the code	Improper Authorization; Protection Mechanism Failure	Android kernel	https://source.android.com/docs/security/bulletin/pixel/2026/2026-09-01	active	no	total
CVE-2026-59160	8,8	Yeger	Missing Authentication for Critical Function	Prior to 2.8.9	https://github.com/DerYeger/yeger/commit/a6c41db6b575cccd8ff89d8e8ce1792ad062852 https://github.com/DerYeger/yeger/releases/tag/@yeger/turbo-graph@2.8.9 https://github.com/DerYeger/yeger/security/advisories/GHSA-2r5q-h53f-9rp3	poc	no	total
CVE-2026-61701	8,8	laravel-magiclink	Deserialization of Untrusted Data	>= 2.0.0, < 2.25.1	https://github.com/cesargb/laravel-magiclink/commit/19fa820a49ea9b3984e9a91b4bf4bf0cf8375183 https://github.com/cesargb/laravel-magiclink/pull/148 https://github.com/cesargb/laravel-magiclink/releases/tag/v2.25.1 https://github.com/cesargb/laravel-magiclink/security/advisories/GHSA-r33w-fg8j-9c94	none	no	total
CVE-2026-79411	8,8	the admin user-management component of Webkul Bagisto	Improper Privilege Management		https://github.com/itsukasanui/bagisto-cve/blob/main/CVE-2026-79411.md	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-2026-82028	8,8	Magistrala	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	before 1.0.0	https://github.com/absmach/magistrala/pull/3581 https://github.com/absmach/magistrala/pull/3581/changes/aac9461aa561c3de7aa9a0dc814ac84c602e0cf9 https://github.com/absmach/magistrala/releases/tag/v1.0.0 https://www.vulncheck.com/advisories/magistrala-sql-injection-via-format-parameter-in-reader-api	none	no	total
CVE-2026-88616	8,8	RuoYi-Vue-Plus	Incorrect Authorization		https://github.com/dromara/RuoYi-Vue-Plus https://github.com/returnwrong/returnwrong-security-advisories/blob/main/CVE-2026-88616.md	poc	no	total
CVE-2026-90777	8,8	ESPnet	Deserialization of Untrusted Data	before 202609	https://github.com/espnet/espnet https://github.com/espnet/espnet/blob/v.202511/espnet2/torch_utils/load_pretrained_model.py#L99 https://github.com/espnet/espnet/commit/91ca045fc179f29bc7b7fe05cd852aea65310003 https://github.com/espnet/espnet/releases/tag/v.202609 https://github.com/espnet/espnet/security/advisories/GHSA-64f6-3ggc-r926 https://www.vulncheck.com/advisories/espnet-before-202609-remote-code-execution-via-unsafe-deserialization	poc	no	total
CVE-2026-91200	8,8	DevSpace	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	through 6.3.21	https://github.com/devspace-sh/devspace https://github.com/devspace-sh/devspace/blob/7f272dcf90653fa9b42bc4347f7f3f9a52b0e8b5/pkg/devspace/sync/tar.go#L68-L82 https://github.com/devspace-sh/devspace/blob/7f272dcf90653fa9b42bc4347f7f3f9a52b0e8b5/pkg/devspace/sync/util.go#L9-L11 https://github.com/devspace-sh/devspace/issues/3290 https://www.vulncheck.com/advisories/devspace-through-6.3.21-path-traversal-via-tar-extraction	none	no	total
CVE-2026-91771	8,8	Weights & Biases wandb	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	before 0.29.0	https://github.com/wandb/wandb https://github.com/wandb/wandb/blob/v0.27.2/wandb/apis/public/files.py#L319-L347 https://github.com/wandb/wandb/commit/e52558f3a6a94ea816af74969a13a35e5904cad6 https://github.com/wandb/wandb/issues/12592 https://github.com/wandb/wandb/releases/tag/v0.29.0 https://www.vulncheck.com/advisories/weights-biases-wandb-before-0.29.0-path-traversal-via-file-download			
CVE-2026-91925	8,8	Polyaxon	Improper Neutralization of Special Elements Used in a Template Engine	through 2.16.4	https://github.com/polyaxon/cli/blob/bfea04a0bf93886f69a3195954204d9d010b55aa/cli/polyaxon/_polyaxonfile/specs/libs/engine.py https://github.com/polyaxon/cli/blob/bfea04a0bf93886f69a3195954204d9d010b55aa/cli/polyaxon/_polyaxonfile/specs/sections.py https://github.com/polyaxon/polyaxon https://github.com/polyaxon/polyaxon/issues/1540 https://www.vulncheck.com/advisories/polyaxon-through-2.16.4-server-side-template-injection-via-unsandboxed-jinja2-engine	poc	no	total
CVE-2026-91964	8,8	FreeRDP versions	Heap-based Buffer Overflow	versions before 3.31.0	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-2yf2-grvi-6q8x https://www.vulncheck.com/advisories/freerdp-2.0.0-through-3.30.0-heap-buffer-overflow-via-routingtoken	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-2026-90943	8,7	parallax filament-comments	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	through 3.0.0	https://github.com/parallax/filament-comments/blob/3.0.0/resources/views/comments.blade.php https://github.com/parallax/filament-comments/blob/3.0.0/src/Policies/FilamentCommentPolicy.php https://hackindex.io/research/stored-xss-filament-comments-unescaped-rendering https://packagist.org/packages/parallax/filament-comments https://www.vulncheck.com/advisories/parallax-filament-comments-through-3.0.0-stored-xss-via-comment-body	none	no	total
CVE-2026-55691	8,6	The EmbedVideo Extension	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Prior to 4.1.0	https://github.com/StarCitizenWiki/mediawiki-extensions-EmbedVideo/commit/370156335b325bb81d14d89edf0a1f2643d50a84 https://github.com/StarCitizenWiki/mediawiki-extensions-EmbedVideo/releases/tag/v4.1.0 https://github.com/StarCitizenWiki/mediawiki-extensions-EmbedVideo/security/advisories/GHSA-7h5p-637f-lfr7	poc	yes	partial
CVE-2026-57586	8,6	CodeRAG	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Prior to 1.3.1	https://github.com/haranor/agent-coderag/commit/1d917513cd95209bab9cbb5fe00df84989805e7d https://github.com/haranor/agent-coderag/releases/tag/v1.3.1 https://github.com/haranor/agent-coderag/security/advisories/GHSA-wq5p-8h9p-3mr7	none	no	total
CVE-2026-59973	8,5	FrontMCP	Server-Side Request Forgery (SSRF)	< 1.5.0; < 2.5.0	https://github.com/agentfront/frontmcp/commit/96a78eaa5c6c4bc51ccd557d83d1a03344cb03d https://github.com/agentfront/frontmcp/pull/496 https://github.com/agentfront/frontmcp/releases/tag/v1.5.0 https://github.com/agentfront/frontmcp/security/advisories/GHSA-65h7-9wrw-629c https://github.com/agentfront/mcp-from-openapi/commit/be3409cce6e97642696d4ee5a4e4e2712490b277 https://github.com/agentfront/mcp-from-openapi/pull/7	poc	no	partial
CVE-2026-54447	8,4	garminconnect	Incorrect Permission Assignment for Critical Resource	Prior to 0.3.5	https://github.com/cyberjunky/python-garminconnect/commit/8256b577190b446e279c81b845d8e27d0ea1fbf5 https://github.com/cyberjunky/python-garminconnect/releases/tag/0.3.5 https://github.com/cyberjunky/python-garminconnect/security/advisories/GHSA-wjhr-76vg-2hvc	none	no	total
CVE-2026-90560	8,2	zstd-jni	Out-of-bounds Read	versions 1.2.0 through 1.5.7-13	https://github.com/luben/zstd-jni https://github.com/luben/zstd-jni/blob/v1.2.0/src/main/java/com/github/luben/zstd/ZstdDictDecompress.java#L37 https://github.com/luben/zstd-jni/blob/v1.5.7-13/src/main/java/com/github/luben/zstd/ZstdDictDecompress.java#L49 https://github.com/luben/zstd-jni/commit/b74ab242d640c40897e62aab4c744ddfad1f915f https://github.com/luben/zstd-jni/issues/405 https://github.com/luben/zstd-jni/releases/tag/v1.5.7-14	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-2026-37008	8,1	CrewAI	Improper Protection of Alternate Path	prior to fb2323b3deb3ec62b3965526857e77a2264e4cd0	https://docs.python.org/3/library/ctypes.html https://github.com/crewAIinc/crewAI/commit/fb2323b3deb3ec62b3965526857e77a2264e4cd0 https://veranngame.com/cves/detail/?slug=crewai-sandbox-escape	poc	no	total
CVE-2026-54076	8,1	ArcadeDB	Missing Authorization; Incorrect Authorization	Prior to 26.6.1	https://github.com/ArcadeData/arcadedb/commit/2ee76fe442b974b2482f1e9eddd1ab429bcac614 https://github.com/ArcadeData/arcadedb/pull/4423 https://github.com/ArcadeData/arcadedb/releases/tag/26.6.1 https://github.com/ArcadeData/arcadedb/security/advisories/GHSA-vq6x-6pg9-6wgq	none	no	total
CVE-2026-59569	8,1	Zscaler Client Connector on Android and ChromeOS	Improper Input Validation	prior to Android: 4.2.0.152; prior to ChromeOS: 4.2.0.152	https://help.zscaler.com/zscaler-client-connector/client-connector-app-release-summary-2026	none	no	total
CVE-2026-79410	8,1	the add-to-cart path of Webkul Bagisto	Improper Input Validation		https://github.com/isukasanui/bagisto-cve/blob/main/CVE-2026-79410.md	poc	no	total
CVE-2026-79425	8,1	the /admin-api/file/online_upload component of CRMEB	Server-Side Request Forgery (SSRF)		https://github.com/crmeh/CRMEB https://github.com/returnwrong/returnwrong-security-advisories/blob/main/CVE-2026-79425.md	poc	no	total
CVE-2026-90651	8,1	registry mode	Improper Certificate Validation	before 2.0.0; versions before 1.1.334	https://docs.socket.dev/docs/registry-mode-configuration-reference https://github.com/SocketDev/socket-registry-firewall/releases/tag/v2.0.0	none	no	partial
CVE-2026-55225	8,0	Strimzi; various deployment configurations	Improper Privilege Management; Unintended Proxy or Intermediary ('Confused Deputy'); Execution with Unnecessary Privileges	1.0.0 and earlier	https://github.com/strimzi/strimzi-kafka-operator/commit/b3bfeffcc30754c3e62e6f4afd8a76942cac440d https://github.com/strimzi/strimzi-kafka-operator/commit/f6c5207ba7ec89b46ce6720b8638d647e556a261 https://github.com/strimzi/strimzi-kafka-operator/pull/12844 https://github.com/strimzi/strimzi-kafka-operator/releases/tag/1.0.1 https://github.com/strimzi/strimzi-kafka-operator/releases/tag/1.1.0 https://github.com/strimzi/strimzi-kafka-operator/security/advisories/GHSA-mw9r-p8xp-wx96	none	no	total
CVE-2026-19624	7,8	NetworkManager-l2tp	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	1.0.0 prior to 1.0.16; 1.2.0 prior to 1.2.22; 1.8.0 prior to 1.8.10; 1.20.0 prior to 1.20.24; 1.52.0 prior to 1.52.4	https://bodhi.fedoraproject.org/updates/?packages=NetworkManager-l2tp https://github.com/nm-l2tp/NetworkManager-l2tp/commit/3704d8c9d5e5f9ed1626a8ce7627a04247cea673 https://github.com/nm-l2tp/NetworkManager-l2tp/commit/95b6b46f48a0c9eabc79272cd313f219110ef91c https://github.com/nm-l2tp/NetworkManager-l2tp/releases https://lennemanlabs.com/posts/nm-l2tp-newline-to-root/	none	no	total
CVE-2026-23789	7,8	MFC in Samsung Mobile Processor and Wearable Processor Exynos	Double Free	2025-12-23 and earlier	https://semiconductor.samsung.com/support/quality-support/product-security-updates/ https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2026-23789/	none	no	total
CVE-2026-90553	7,8	vLLM	Improper Control of Generation of Code ('Code Injection')	before 0.28.0	https://github.com/vllm-project/vllm/security/advisories/GHSA-3c86-2m5g-59a7 https://www.vulncheck.com/advisories/vllm-before-0.28.0-remote-code-execution-via-lavaonevision2-processor	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-2026-90556	7,8	FreeCiv versions	Heap-based Buffer Overflow	versions before 3.2.6	https://github.com/freeciv/freeciv https://github.com/freeciv/freeciv/blob/R3_2_5/server/savegame/savegame2.c#L788 https://github.com/freeciv/freeciv/blob/R3_2_5/server/savegame/savegame3.c#L964 https://github.com/freeciv/freeciv/commit/75ecde3e86ddf2fe775768450e9a290a4f4d4387 https://github.com/freeciv/freeciv/releases/tag/R3_2_6 https://redmine.freeciv.org/issues/2161			
CVE-2026-90783	7,8	MKVToolNix	Integer Overflow to Buffer Overflow	through 101.0	https://codeberg.org/mbunkus/mkvtoolnix https://codeberg.org/mbunkus/mkvtoolnix/commit/1495126138e086080f0163bee27fafbdf956a1d0 https://codeberg.org/mbunkus/mkvtoolnix/src/tag/release-101.0/lib/avilib-0.6.10/avilib.c#L2552-L2570 https://www.vulncheck.com/advisories/mkvtoolnix-through-101.0-heap-buffer-overflow-via-avilib-odml-superindex-integer-wraparound	none	no	total
CVE-2026-90894	7,8	Parallels Desktop for Mac	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'); Improper Neutralization of Argument Delimiters in a Command ('Argument Injection'); Improper Privilege Management	26.4.0	https://kb.parallels.com/en/131168 https://www.parallels.com/products/desktop/	none	no	total
CVE-2026-19499	7,7	the GNU C Library	Heap-based Buffer Overflow	version 2.38 to 2.44	https://sourceware.org/bugzilla/show_bug.cgi?id=34510 https://sourceware.org/git/?p=glibc.git;a=blob_plain;f=advisories/GLIBC-SA-2026-0017	none	no	partial
CVE-2026-31278	7,7	the /api/v2/setting/adserversetting endpoint of Suprema BioStar	Cleartext Transmission of Sensitive Information	before 2.9.12; before 1.0.2	https://github.com/mda1r/biostar2-ad-credential-exposure https://www.supremainc.com https://github.com/mda1r/CVE-2026-31278	poc	no	partial
CVE-2026-47701	7,7	The OpenTelemetry Operator	Exposure of Sensitive Information to an Unauthorized Actor	Prior to 0.152.0	https://github.com/open-telemetry/opentelemetry-operator/commit/95a8c2a3dc64a762d3ab8eba8c903b5702a03a9c https://github.com/open-telemetry/opentelemetry-operator/pull/5104 https://github.com/open-telemetry/opentelemetry-operator/releases/tag/v0.152.0 https://github.com/open-telemetry/opentelemetry-operator/security/advisories/GHSA-cxh2-4639-vmc5	none	no	partial
CVE-2026-53957	7,7	Contentful MCP Server	Server-Side Request Forgery (SSRF)	< 1.7.19; < 0.4.5	https://github.com/contentful/contentful-mcp-server/commit/fa7477ee48515f4248bc91a025eab0ca83423fe0 https://github.com/contentful/contentful-mcp-server/pull/376 https://github.com/contentful/contentful-mcp-server/releases/tag/mcp-server@1.7.19 https://github.com/contentful/contentful-mcp-server/releases/tag/mcp-tools@0.4.5 https://github.com/contentful/contentful-mcp-server/security/advisories/GHSA-2xhq-73j7-rrqx			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-54155	7,7	node-opcua	Improper Verification of Cryptographic Signature	Prior to 2.166.0	https://github.com/node-opcua/node-opcua/commit/c6b05738682f5c8d70b1ea275c881f01a1cd9787 https://github.com/node-opcua/node-opcua/releases/tag/v2.166.0 https://github.com/node-opcua/node-opcua/security/advisories/GHSA-mg36-523m-x7vy	none	no	total
CVE-2026-55253	7,7	LangChain MongoDB	Improper Neutralization of Special Elements in Data Query Logic	< 0.4.0; < 0.3.0	https://github.com/langchain-ai/langchain-mongodb/commit/14a6cc39e67d23fd409cd13a9caae2c329df0a09 https://github.com/langchain-ai/langchain-mongodb/commit/240e7ecee432ea006d9fef6ea506bfd2e009a3f4 https://github.com/langchain-ai/langchain-mongodb/commit/5465e4d3ea0ef5c88a666a6442bd853ff4bd70e5 https://github.com/langchain-ai/langchain-mongodb/pull/384 https://github.com/langchain-ai/langchain-mongodb/releases/tag/libs/langgraph-checkpoint-mongodb/v0.4.0 https://github.com/langchain-ai/langchain-mongodb/releases/tag/libs/langgraph-store-mongodb/v0.3.0	none	no	partial
CVE-2026-73496	7,7	MCP Atlassian	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'); External Control of File Name or Path	Prior to 0.22.0	https://github.com/sooperset/mcp-atlassian/commit/b041733473f95119dd539542a43c280737a8e460 https://github.com/sooperset/mcp-atlassian/pull/1448 https://github.com/sooperset/mcp-atlassian/releases/tag/v0.22.0 https://github.com/sooperset/mcp-atlassian/security/advisories/GHSA-wm45-qh3g-v83f	poc	no	partial
CVE-2026-76820	7,7	OpenCTI	Server-Side Request Forgery (SSRF)	Prior to 7.260701.0	https://github.com/OpenCTI-Platform/opentcti/commit/6c1114ce8ce8f3a9d9b8c82dff3a3a462e5dc1f https://github.com/OpenCTI-Platform/opentcti/pull/16617 https://github.com/OpenCTI-Platform/opentcti/releases/tag/7.260701.0 https://github.com/OpenCTI-Platform/opentcti/security/advisories/GHSA-f6pj-3m32-g934	none	no	partial
CVE-2026-90769	7,7	Open Notebook	Server-Side Request Forgery (SSRF)	before 1.11.0	https://github.com/lfnovo/open-notebook/blob/8889087e317177d7b6e286342ab34e0c9c01d43e/api/routers/sources.py https://github.com/lfnovo/open-notebook/commit/9045ea50196927eac7de647bb5b7009349236fb4 https://github.com/lfnovo/open-notebook/issues/1284 https://www.vulncheck.com/advisories/open-notebook-before-1.11.0-server-side-request-forgery-via-link-source	poc	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-2026-91923	7,7	KubeSphere	Server-Side Request Forgery (SSRF)	through 4.1.3	https://github.com/kubesphere/kubesphere https://github.com/kubesphere/kubesphere/blob/3ef3a6bc98b790480577e87fbc75bee5b3438862/config/kube-core/templates/globalroles.yaml https://github.com/kubesphere/kubesphere/blob/3ef3a6bc98b790480577e87fbc75bee5b3438862/pkg/kapis/resources/v1alpha2/handler.go https://github.com/kubesphere/kubesphere/blob/3ef3a6bc98b790480577e87fbc75bee5b3438862/pkg/model/s/qit/qit.go https://github.com/kubesphere/kubesphere/issues/6653 https://www.vulncheck.com/advisories/kubesphere-through-4.1.3-ssrf-via-git-credential-verification-endpoint			
CVE-2026-54087	7,6	EasyAdmin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'); Unrestricted Upload of File with Dangerous Type	>= 5.0.0, < 5.0.13	https://github.com/EasyCorp/EasyAdminBundle/commit/8132b2b0ca3876c9261264fa267106a1b2c10a68 https://github.com/EasyCorp/EasyAdminBundle/releases/tag/v5.0.13 https://github.com/EasyCorp/EasyAdminBundle/security/advisories/GHSA-8559-gw3-q37r	none	no	partial
CVE-2026-90772	7,6	Amundsen frontend	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	through 4.3.0	https://github.com/amundsen-io/amundsen https://github.com/amundsen-io/amundsen/blob/frontend-4.3.0/frontend/amundsen_application/static/js/components/ResourceListItem/TableListItem/index.tsx https://github.com/amundsen-io/amundsen/issues/2362 https://www.vulncheck.com/advisories/amundsen-frontend-through-4.3.0-stored-xss-via-description	poc	no	partial
CVE-2025-66974	7,5	Prolink 13A Smart Plug Model	Improper Input Validation		https://github.com/Anonymous241429/crossprobe https://prolink2u.com/collections/data?filter.p.m.custom.filter_category=Smart+Home	none	yes	partial
CVE-2026-28960	7,5	iPadOS	Improper Input Validation	versions up to (excluding) 18.7.10	https://support.apple.com/en-us/148287	none	yes	partial
CVE-2026-50270	7,5	dd-trace-java	Allocation of Resources Without Limits or Throttling	Prior to 1.62.0	https://github.com/DataDog/dd-trace-java/commit/16c6a5fd1fed71cef6c35f69122f19f5ee242757 https://github.com/DataDog/dd-trace-java/pull/11265 https://github.com/DataDog/dd-trace-java/releases/tag/v1.62.0 https://github.com/DataDog/dd-trace-java/security/advisories/GHSA-74xj-wh4w-vqxc	none	yes	partial
CVE-2026-51134	7,5	The C-MOR Video Surveillance web interface (up to	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	up to version 6.0104)	https://albcyberguards.com/blog/cve-2026-51134-c-mor-path-traversal https://www.c-mor.com/video-surveillance-info/video-surveillance-change-log	poc	yes	partial
CVE-2026-53752	7,5	docx4j	Uncontrolled Recursion; Allocation of Resources Without Limits or Throttling	Prior to 11.5.14	https://github.com/plutext/docx4j/commit/47b528c7dd4c81bcfc8e7fe9df7610c60446f95f https://github.com/plutext/docx4j/commit/e06cafb334089f0be02e1c63a7c0a602bd44bf06 https://github.com/plutext/docx4j/releases/tag/docx4j-11.5.14 https://github.com/plutext/docx4j/security/advisories/GHSA-qc95-3vw8-vq43	none	yes	partial
CVE-2026-54567	7,5	Flask-Reuploaded	Improper Handling of Case Sensitivity; Unrestricted Upload of File with Dangerous Type	< 1.6.0	https://github.com/iugmac00/flask-reuploaded/commit/5ded76092429c6eb8a4af941b14fbde40a38fff4 https://github.com/iugmac00/flask-reuploaded/pull/186 https://github.com/iugmac00/flask-reuploaded/security/advisories/GHSA-937x-gpqr-72qg	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-2026-55149	7,5	Vouch Proxy	Memory Allocation with Excessive Size Value	Prior to 0.48.0	https://github.com/vouch/vouch-proxy/commit/fa18ce30ba50a4863a436acad044c22965329c4f https://github.com/vouch/vouch-proxy/releases/tag/v0.48.0 https://github.com/vouch/vouch-proxy/security/advisories/GHSA-qgff-5854-px68			
CVE-2026-55178	7,5	GeoLens	Exposure of Sensitive Information to an Unauthorized Actor; Authorization Bypass Through User-Controlled Key; Missing Authorization	Prior to 1.2.3	https://github.com/geolens-io/geolens/commit/01bc87da03a5ecd0322c42388f4bfc7cb2ed06 https://github.com/geolens-io/geolens/commit/07dfb1c63ecfc065c0c47b7718ec6e97798b1e https://github.com/geolens-io/geolens/commit/2c031da8e753639ff0e36d47ca05bb96f9e4a9e https://github.com/geolens-io/geolens/commit/31a103b96b9fd6ad90308b3e27a581852c4a69bd https://github.com/geolens-io/geolens/commit/407c068836058fdeca6bb477d39f841316b326a5 https://github.com/geolens-io/geolens/pull/234			
CVE-2026-57129	7,5	PraisonAI	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	< 1.6.59	https://github.com/MervinPraison/PraisonAI/commit/b4270173d4123fb1ee8910588f0896668ee21b59 https://github.com/MervinPraison/PraisonAI/releases/tag/v4.6.59 https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-2rcq-mm5h-xchx	poc	yes	partial
CVE-2026-58483	7,5	mcp-searxng	Uncontrolled Resource Consumption	Prior to 1.7.1	https://github.com/ihor-sokoluk/mcp-searxng/commit/f5a947ed1650daed10fbdcd53c0db5a86489ffe4 https://github.com/ihor-sokoluk/mcp-searxng/pull/121 https://github.com/ihor-sokoluk/mcp-searxng/releases/tag/v1.7.1 https://github.com/ihor-sokoluk/mcp-searxng/security/advisories/GHSA-xcqx-9jf5-w339	poc	yes	partial
CVE-2026-89025	7,5	Hirschmann HiOS Switch Platform devices; the integrated web server due to missing validation of HTTP(S) content	Improper Handling of Exceptional Conditions	07.0.0 through 07.1.11; 08.0.0 through 08.7.09; 09.0.00 through 09.0.12; 09.3.00 through 09.3.02; 10.0.0 through 10.3.07; 10.4.00; 10.5.00	https://assets.belden.com/asset/2ba884e3-c0c9-40f6-aa22-a9e852b20af4/PSIRT-6_HTTPS_Vulnerability_HiOS.pdf https://www.vulncheck.com/advisories/hirschmann-hios-switch-platform-dos-via-malformed-http-request	none	yes	partial
CVE-2026-90559	7,5	snappy-java	Out-of-bounds Write	through 1.1.10.8	https://github.com/xerial/snappy-java https://github.com/xerial/snappy-java/blob/v1.1.10.8/src/main/java/org/xerial/snappy/Snappy.java#L561 https://github.com/xerial/snappy-java/issues/728 https://www.vulncheck.com/advisories/snappy-java-through-1.1.10.8-out-of-bounds-write-via-uncompress	none	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-2026-90776	7,5	Nodemailer	Inefficient Algorithmic Complexity	versions 9.1.0 through 10.0.4	https://github.com/nodemailer/nodemailer https://github.com/nodemailer/nodemailer/blob/v10.0.4/src/addressparser/index.ts#L251 https://github.com/nodemailer/nodemailer/commit/c07f17518d25aca8ab2ad66968dcbca538c24b89 https://github.com/nodemailer/nodemailer/releases/tag/v10.0.5 https://github.com/nodemailer/nodemailer/security/advisories/GHSA-prgh-xp8r-p3m5 https://www.vulncheck.com/advisories/nodemailer-9.1.0-through-10.0.4-denial-of-service-via-quadratic-address-parsing	poc	yes	partial
CVE-2026-90946	7,5	DeepWiki-Open through commit d92819a; the unauthenticated /ws/chat Web-Socket endpoint that accepts repo_url as a filesystem path with no containment	External Control of File Name or Path	d92819a and earlier	https://github.com/AsyncFuncAI/deepwiki-open https://github.com/AsyncFuncAI/deepwiki-open/blob/16f35a0fc0284e99b7963bbf4e8585e9957e2fe1/api/data_pipeline.py https://github.com/AsyncFuncAI/deepwiki-open/blob/d92819a9c9f3b99416e3580ff235fc9d3adf8b89/api/repository.py https://github.com/AsyncFuncAI/deepwiki-open/issues/536 https://www.vulncheck.com/advisories/deepwiki-open-through-commit-d92819a-arbitrary-file-read-via-ws-chat-websocket	poc	yes	partial
CVE-2026-91144	7,5	ZFile	Authorization Bypass Through User-Controlled Key	through 5.0.5	https://github.com/zfile-dev/zfile https://github.com/zfile-dev/zfile/blob/5.0.5/src/main/java/im/zhaojun/zfile/module/share/service/ShareLinkFileService.java https://github.com/zfile-dev/zfile/issues/826 https://www.vulncheck.com/advisories/zfile-through-5.0.5-share-entry-filter-bypass-via-download-endpoint			
CVE-2026-91752	7,5	GNU libextractor	Memory Allocation with Excessive Size Value	before 1.15; up to 4	https://git.qnunet.org/qnunet/libextractor/commit/04004eb19033e093938138b09befdf31e71e8522.html https://git.qnunet.org/qnunet/libextractor/commit/2781c7e9095f4ddaff4f535d69342f3903b18422.html https://github.com/Haitam-lazaar/libextractor-ole2-rce https://www.gnu.org/software/libextractor/ https://www.vulncheck.com/advisories/gnu-libextractor-before-1.15-stack-overflow-via-ole2 http://www.openwall.com/lists/oss-security/2026/09/16/16			
CVE-2026-91947	7,5	FreeRDP server versions	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	versions before 3.31.0	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6mpx-c8ri-whj5 https://www.vulncheck.com/advisories/freerdp-server-before-3.31.0-use-after-free-via-drdrnvc	none	no	total
CVE-2026-91996	7,5	lamp-cloud	Missing Authentication for Critical Function	through 5.10.0	https://github.com/dromara/lamp-cloud https://github.com/dromara/lamp-cloud/blob/bdc1a406eb0f6291e9f6dbad9cbccd67bc6a37b6/lamp-generator/lamp-generator-controller/src/main/java/top/tangyh/lamp/generator/controller/DefGenProjectController.java#L61-L64 https://github.com/dromara/lamp-cloud/blob/bdc1a406eb0f6291e9f6dbad9cbccd67bc6a37b6/lamp-public/lamp-common/src/main/java/top/tangyh/lamp/common/properties/IgnoreProperties.java#L88 https://github.com/qeo-chen/oss/blob/main/lamp-cloud.md https://www.vulncheck.com/advisories/lamp-cloud-through-5.10.0-missing-authentication-for-ivm-properties-endpoint			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-73494	7,4	blaze	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')	Prior to 0.23.18	https://github.com/http4s/blaze/commit/3f7c022e306631b006dcb43a1d7f65c0d1966f17 https://github.com/http4s/blaze/commit/4eec2007806a99acfebf00ebb636ddc39a147a96 https://github.com/http4s/blaze/commit/927b67753a78c13c4445dac9307f511f5c4878c3 https://github.com/http4s/blaze/commit/a54bc9cd31758335c7f24e29763622fd03fcf734 https://github.com/http4s/blaze/commit/c47d9675f87603f11b32a11d503626bdf9be5c7a https://github.com/http4s/blaze/commit/e871ebb1d27f50c98fd56988526ce42d0fee74d6	none	no	total
CVE-2026-90647	7,4	ASE2000 V2 Communication Test Set	Improper Certificate Validation	2.35 through 2.37	https://www.ase-systems.com/wp-content/uploads/2026/07/CYB_2026_86278_Advisory_v1.0.pdf	none	no	total
CVE-2024-58383	7,3	Froxlor	Incorrect Permission Assignment for Critical Resource	before 2.2.0; up to and including 2.2.0-rc3)	https://github.com/froxlor/froxlor/security/advisories/GHSA-34gg-65m4-f23m https://www.vulncheck.com/advisories/froxlor-before-2.2.0-insecure-file-permissions-mysql-conf			
CVE-2026-91145	7,1	Activiti	Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	through 7.1.0.M6	https://github.com/Activiti/Activiti https://github.com/Activiti/Activiti/blob/7.1.0.M6/activiti-core/activiti-api-impl/activiti-api-process-runtime-impl/src/main/java/org/activiti/runtime/api/impl/ExpressionResolver.java https://github.com/Activiti/Activiti/blob/7.1.0.M6/activiti-core/activiti-engine/src/main/java/org/activiti/engine/impl/bpmn/behavior/MailActivityBehavior.java https://github.com/Activiti/Activiti/issues/5438 https://www.vulncheck.com/advisories/activiti-through-7.1.0-m6-expression-injection-via-mail-task	poc	no	partial

CISA/CERT-EU Alerts & Advisories

Αυτό το κομμάτι περιλαμβάνει ειδοποιήσεις από επίσημες πηγές, κυρίως CISA και CERT-EU, σχετικά με κρίσιμες ευπάθειες ή ενεργές απειλές. Συνήθως αφορούν βιομηχανικά ή κρίσιμα συστήματα, αλλά και mainstream λογισμικό. Προσφέρονται σε μορφή σύντομων αναφορών και οδηγούν σε πιο λεπτομερείς τεχνικές οδηγίες.

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds One Known Exploited Vulnerability to Catalog CISA	CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog , based on evidence of active exploitation.	https://cisa.gov/news-events/alerts/2026/09/14/cisa-adds-one-known-exploited-vulnerability-catalog

News

Η ενότητα "News" συνοψίζει τα πιο σημαντικά γεγονότα της εβδομάδας στον τομέα της κυβερνοασφάλειας. Εδώ θα βρείτε επιθέσεις που ξεχώρισαν, νέες τεχνικές που εντοπίστηκαν, ή ενέργειες από γνωστές ομάδες hacking. Δίνει την απαραίτητη εικόνα του τι συμβαίνει διεθνώς και πού πρέπει να στραφεί η προσοχή.

Σύντομη περιγραφή / Τίτλος	URL
Malicious Admin Menu Editor Pro plugin backdoors 1,500 WordPress sites	https://bleepingcomputer.com/news/security/malicious-admin-menu-editor-pro-plugin-backdoors-1-500-wordpress-sites
“We Think the Security Control Is Working” Is No Longer Good Enough	https://securityweek.com/we-think-the-security-control-is-working-is-no-longer-good-enough
CISA and NIST Release Technical Checklist for Safeguarding Identity Tokens From Theft and Misuse	https://cybersecuritynews.com/cisa-nist-identity-token-security
VectraRAT Can Hack Windows Enterprises for \$250 per Month	https://darkreading.com/endpoint-security/vectrarat-hack-windows-enterprises
CenterPoint Energy confirms customer data stolen in cyberattack	https://bleepingcomputer.com/news/security/centerpoint-energy-confirms-customer-data-stolen-in-cyberattack
CISA Shares 17 Techniques Used by Hackers to Compromise Active Directory Environments	https://cybersecuritynews.com/cisa-active-directory-attack-techniques
Most Fraudulent Hires Receive Credentials Before Detection	https://infosecurity-magazine.com/news/fraudulent-hires-credentials
Hackers target WordPress sites via third-party WooCommerce plugin	https://bleepingcomputer.com/news/security/hackers-target-wordpress-sites-via-third-party-woocommerce-plugin
Black Axe Members Extradited to US Over Internet Fraud Claims	https://infosecurity-magazine.com/news/black-axe-members-extradited-us
AI the Top Priority for New Spend as Cyber Budgets Flatline	https://infosecurity-magazine.com/news/ai-top-priority-new-spend-cyber
Microsoft Confirms KB5002914 Update Breaks Copy and Paste on Excel	https://cybersecuritynews.com/kb5002914-update-breaks-copy-paste
Microsoft releases emergency Windows updates to fix RDS failures	https://bleepingcomputer.com/news/microsoft/microsoft-releases-emergency-windows-updates-to-fix-rds-failures
Homebrew 7.0.0 gets built-in GUI, better security controls	https://bleepingcomputer.com/news/security/homebrew-700-gets-built-in-gui-better-security-controls
New DDROP Attack Breaks Intel TDX and AMD SEV-SNP Confidential Computing	https://thehackernews.com/2026/09/new-ddrop-attack-breaks-intel-tdx-and.html
WordPress Adds Automated Plugin Reviews to Block High-Risk Updates Before Distribution	https://thehackernews.com/2026/09/wordpress-adds-automated-plugin-reviews.html
Malicious Twitch Extension Exposes 31,000 Users' OAuth Tokens	https://infosecurity-magazine.com/news/malicious-twitch-extension-oauth
Defense Cyber Spending Set to Surge Amid Rising Attacks on Military Systems	https://infosecurity-magazine.com/news/defense-cyber-spending-attacks
AI Changed the Exposure Problem. Validation Needs to Change With It.	https://thehackernews.com/2026/09/ai-changed-exposure-problem-validation.html
Microsoft: September updates cause RDS failures on Windows Server	https://bleepingcomputer.com/news/microsoft/microsoft-september-updates-cause-rds-failures-on-windows-server
OpenAI Agent Swarm Hacks RubyGems Package Manager	https://infosecurity-magazine.com/news/openai-agent-swarm-hacks-rubygems

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
Revolut Data Breach Via Fake Government Requests - What We Know So Far	https://cybersecuritynews.com/fintech-revolut-data-breach
Revolut Confirms Data Breach Through Fake Government Requests	https://infosecurity-magazine.com/news/revolut-data-breach-fake-government
Revolut Data Breach Exposes Customers' Passport Copies and Full Transaction Histories to Hackers	https://cybersecuritynews.com/revolut-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
\$1 Million Sandbox Challenge Uncovers Linux Kernel Flaws	https://securityweek.com/1-million-sandbox-challenge-uncovers-linux-kernel-flaws
Apple Rolls Out Massive Security Update Fixing 273 Vulnerabilities Across Its Devices	https://cybersecuritynews.com/apple-security-update-273-vulnerabilities
Human Attacker Exploits Marimo RCE, Reaches SSH Bastion in Eight Seconds	https://thehackernews.com/2026/09/human-attacker-exploits-marimo-rce.html
Mass-Scanning Campaign Exploits Vite Flaw to Extract Cloud Credentials From Exposed Dev Servers	https://thehackernews.com/2026/09/mass-scanning-campaign-exploits-vite.html
Microsoft Releases Emergency Patch to Fix RDS Vulnerability	https://infosecurity-magazine.com/news/microsoft-releases-emergency-patch
LiteSpeed Enterprise Flaw Could Let One Hosting Account Gain Root Access on a Shared Server	https://thehackernews.com/2026/09/litespeed-enterprise-flaw-could-let-one.html
Cisco Secure Email Gateway Flaw Exploited in the Wild, Enables Root Command Execution	https://thehackernews.com/2026/09/cisco-secure-email-gateway-flaw.html
China-Linked Hackers Exploit Chrome-Windows Zero-Day Chain to Deploy GRIMWEDGE	https://thehackernews.com/2026/09/china-linked-hackers-exploit-chrome.html
Root RCE Zero-Day in Cisco Secure Email Gateway Under Active Exploitation	https://securityweek.com/root-rce-zero-day-in-cisco-secure-email-gateway-under-active-exploitation
'Sandworm' Chains Cisco Flaws to Deploy Cyclops Blink	https://darkreading.com/cyberattacks-data-breaches/sandworm-chains-cisco-vulnerabilities-cyclops-blink
Japan's Digital Agency says VPN flaw exposed 246,000 personnel records	https://bleepingcomputer.com/news/security/japans-digital-agency-says-vpn-flaw-exposed-246-000-personnel-records
Maximum Severity GitLab Flaw Puts Supply Chains at Risk	https://darkreading.com/cyberattacks-data-breaches/maximum-severity-gitlab-flaw-supply-chains-risk

Σύντομη περιγραφή / Τίτλος	URL
Telegram Desktop Flaw Lets Hidden JavaScript Exfiltrate Messages From HTML Exports	https://thehackernews.com/2026/09/telegram-desktop-flaw-lets-hidden.html
Hackers Exploit FortiGate SSL-VPN Vulnerability to Attack Broadband Provider	https://cybersecuritynews.com/fortigate-ssl-vpn-vulnerability
Red Heron Exploits Gitea RCE to Compromise 13 Organizations Across Six Countries	https://thehackernews.com/2026/09/red-heron-exploits-gitea-rce-to.html
Human Attacker Hits Machine-Speed Exploitation of Marimo RCE	https://infosecurity-magazine.com/news/human-attacker-machine-speed
Chinese Hackers Exploit Critical Tencent Software Flaw for One-Click Code Execution	https://securityweek.com/chinese-hackers-exploit-critical-tencent-software-flaw-for-one-click-code-execution
Hackers Exploit Maximum Severity Flaw in GitLabs	https://infosecurity-magazine.com/news/hackers-exploit-maximum-severity
CISA Adds 5 Actively Exploited Artifactory, ScreenConnect, and RouterOS Flaws to KEV	https://thehackernews.com/2026/09/cisa-adds-5-actively-exploited.html
Dutch NCSC: Critical Check Point VPN flaws exploitation is imminent	https://bleepingcomputer.com/news/security/dutch-ncsc-critical-check-point-vpn-flaws-exploitation-is-imminent

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 Issues Emergency Fixes After Massive Patch Tuesday	https://darkreading.com/application-security/microsoft-emergency-fixes-patch-tuesday
Apple Patches 200 Vulnerabilities With New iOS 27, macOS Golden Gate 27 Releases	https://securityweek.com/apple-patches-200-vulnerabilities-with-new-ios-27-macos-golden-gate-27-releases
Microsoft Confirms Remote Desktop Services Might Stop Working Following Sept. 2026 Security Update	https://cybersecuritynews.com/remote-desktop-services-stop-working
ConnectWise Patches ScreenConnect Vulnerability Exploited in Worm-Like Attacks	https://securityweek.com/connectwise-patches-screenconnect-vulnerability-exploited-in-worm-like-attacks

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
BambooToken malware controls Windows and Linux systems via MQTT	https://bleepingcomputer.com/news/security/bambootoken-malware-controls-windows-and-linux-systems-via-mqtt
Most Firms Unable to Recover Quickly from Ransomware	https://infosecurity-magazine.com/news/four-of-800-clients-hit-ransomware
Hackers hijack HBO Max Reddit account to push malware in ClickFix ads	https://bleepingcomputer.com/news/security/hackers-hijack-hbo-max-reddit-account-to-push-malware-in-clickfix-ads
3BB Attacker Used MeshCentral Backdoor for Root Access, Targeted Subscriber Credentials	https://thehackernews.com/2026/09/3bb-attacker-used-meshcentral-backdoor.html
⚡ Weekly Recap: Rogue AI Agents, WeChat Worm, PaperCut Attacks, AI Espionage, and Rootkits	https://thehackernews.com/2026/09/weekly-recap-rogue-ai-agents-wechat.html
Three JFrog Artifactory Flaws Exploited for Backdoor Deployment	https://securityweek.com/three-jfrog-artifactory-flaws-exploited-for-backdoor-deployment

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
How to Keep Malware's Rotating Infrastructure From Becoming a Detection Gap	https://cybersecuritynews.com/how-to-keep-malwares-rotating-infrastructure-from-becoming-a-detection-gap
How to Evaluate a Unified Security Platform Using a One-Incident Test	https://thehackernews.com/expert-insights/2026/09/how-to-evaluate-unified-security.html

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 12/09/2026–15/09/2026, 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/