

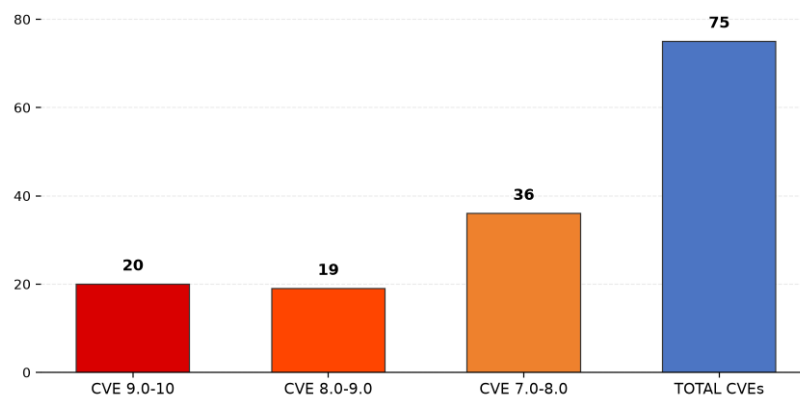


Newsletter on system vulnerabilities and cybersecurity news.

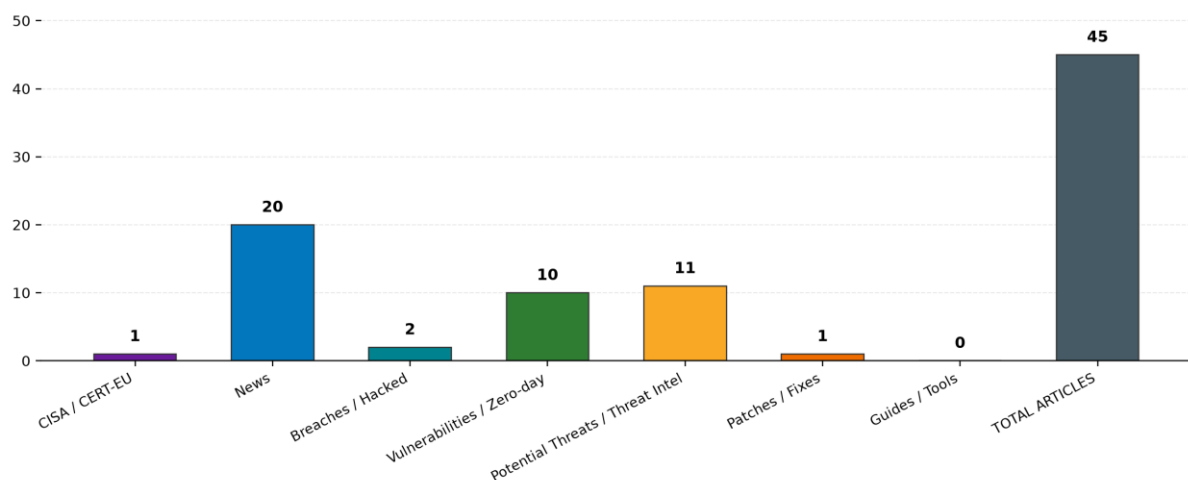
National Cyber Security Authority (NCSA)

Date: 29/08/2026 - 01/09/2026

of CVEs per CVSS score



of articles per section



Contents

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

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-2026-81779	10,0	Newspapers X	Improper Validation of Specified Quantity in Input	from 1.0.46 through 1.0.48.	https://patchstack.com/database/wordpress/theme/newspapers-x/vulnerability/wordpress-newspapers-x-theme-1-0-46-1-0-48-backdoor-vulnerability?_s_id=cve			
CVE-2026-81780	10,0	Hash Form	Unrestricted Upload of File with Dangerous Type	<= 1.4.2	https://patchstack.com/database/wordpress/plugin/hash-form/vulnerability/wordpress-hash-form-plugin-1-4-2-arbitrary-file-upload-vulnerability?_s_id=cve			
CVE-2026-82456	10,0	argocd-mcp	Binding to an Unrestricted IP Address	0.8.0 prior to 0.9.0	https://github.com/argoproj-labs/mcp-for-argocd https://github.com/argoproj-labs/mcp-for-argocd/security/advisories/GHSA-rp45-5x3v-48mr https://www.vulncheck.com/advisories/argocd-mcp-0.8.0-authentication-bypass-via-unauthenticated-http			
CVE-2026-82970	10,0	WP Legal Pages WP Cookie Notice for GDPR, CCPA & ePrivacy Consent	Unrestricted Upload of File with Dangerous Type	through 4.4.1.	https://patchstack.com/database/wordpress/plugin/gdpr-cookie-consent/vulnerability/wordpress-wp-cookie-notice-for-gdpr-ccpa-privacy-consent-plugin-4-4-1-arbitrary-file-upload-vulnerability?_s_id=cve	none	yes	total
CVE-2026-82971	10,0	QVidium Opera11	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'); Improper Neutralization of Special Elements used in a Command ('Command Injection')	3.3.2a26-Ax4x-opera11	https://uxbyw62qm.feishu.cn/wiki/Tn2evwwaafqfabkMWJJcc3rhnd?from=from_copylink https://vuldb.com/cve/CVE-2026-82971 https://vuldb.com/submit/880050 https://vuldb.com/vuln/397334 https://vuldb.com/vuln/397334/cti			
CVE-2026-79748	9,9	MCPHub	Missing Authorization	Prior to version 0.12.15	https://github.com/samanhappy/mcphub/pull/770 https://github.com/samanhappy/mcphub/releases/tag/v0.12.15 https://github.com/samanhappy/mcphub/security/advisories/GHSA-mx89-jix9-qir8	poc	no	total
CVE-2026-82874	9,9	ToolJet	Authorization Bypass Through User-Controlled Key	before v3.16.208	https://github.com/ToolJet/ToolJet/security/advisories/GHSA-w3hx-rq9q-mw5c https://www.vulncheck.com/advisories/tooljet-before-3.16.208-cross-tenant-authorization-bypass-via-tooljet-db	none	no	partial
CVE-2026-82954	9,9	Dokploy	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	up to 0.29.7.	https://vuldb.com/cve/CVE-2026-82954 https://vuldb.com/submit/879844 https://vuldb.com/vuln/397303 https://vuldb.com/vuln/397303/cti			
CVE-2026-83524	9,9	RedPort Optimizer wXa-203, Optimizer wXa-213 and Optimizer wXa-223	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'); Improper Neutralization of Special Elements used in a Command ('Command Injection')	up to 20260704.	https://uxbyw62qm.feishu.cn/wiki/EA4TwFTx0ih9lhkJX5QcnCmlnSd?from=from_copylink https://vuldb.com/cve/CVE-2026-83524 https://vuldb.com/submit/880051 https://vuldb.com/vuln/397374 https://vuldb.com/vuln/397374/cti			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-83772	9,9	Cobham SATCOM VSAT7090 Maritime Satellite Router	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'); Improper Neutralization of Special Elements used in a Command ('Command Injection')	up to 20260704.	https://uxbyw62gm.feishu.cn/wiki/ERqwyvUVfiUM2lkfVwc1swknXg?from=from_copylink https://vuldb.com/cve/CVE-2026-83772 https://vuldb.com/submit/880057 https://vuldb.com/vuln/397501 https://vuldb.com/vuln/397501/ctj			
CVE-2026-58574	9,8	Dell PowerStore	Missing Authentication for Critical Function	prior to 4.1.0.6-2771237 or later; prior to 4.3.1.2-2771239 or later	https://www.dell.com/support/kbdoc/en-us/000497829/dsa-2026-330-dell-powerstore-t-security-update-for-multiple-vulnerabilities	none	yes	total
CVE-2026-75865	9,8	WPLP Cookie Consent – Cookie Banner & Consent Management for GDPR, CCPA & Google Consent Mode	Unrestricted Upload of File with Dangerous Type	up to, and including, 4.4.1.	https://plugins.trac.wordpress.org/changeset/3674117/qdpr-cookie-consent https://www.wordfence.com/threat-intel/vulnerabilities/id/96a2a552-e73f-4b27-88de-50eb63a8d131?source=cve			
CVE-2026-82226	9,8	Tickera	Deserialization of Untrusted Data	<= 3.6.0.2	https://patchstack.com/database/wordpress/plugin/tickera-event-ticketing-system/vulnerability/wordpress-tickera-plugin-3-6-0-2-php-object-injection-vulnerability?_s_id=cve			
CVE-2026-82448	9,8	Shinobi before commit; the child node service that	Use of Hard-coded Credentials	prior to 5a76c74f3977661ff3f9fd55a260db352c0b19c0	https://gitlab.com/Shinobi-Systems/Shinobi/-/blob/04e685b8bd4c6190fcd62993131b86a76c2b806/libs/childNode/utlis.js https://gitlab.com/Shinobi-Systems/Shinobi/-/commit/5a76c74f3977661ff3f9fd55a260db352c0b19c0 https://gitlab.com/Shinobi-Systems/Shinobi/-/merge_requests/554 https://www.vulncheck.com/advisories/shinobi-before-commit-5a76c74f-arbitrary-database-query-execution-via-hardcoded-child-node-key	none	yes	total
CVE-2026-82854	9,8	Nodemailer	Improper Neutralization of CRLF Sequences ('CRLF Injection')	before 8.0.4	https://github.com/nodemailer/nodemailer/security/advisories/GHSA-c7w3-x93f-qmm8 https://www.vulncheck.com/advisories/nodemailer-before-8.0.3-smtp-command-injection-via-envelope-size	none	yes	total
CVE-2026-82859	9,8	hulumi versions	Improper Access Control	versions before v1.3.2	https://github.com/kerberosmansour/hulumi/security/advisories/GHSA-86q4-r5j3-ff5c https://www.vulncheck.com/advisories/hulumi-before-1.3.2-scp-template-tag-on-create-bypass	none	yes	total
CVE-2026-49003	9,6	ZXDU68 S202 V5.0	Improper Authentication	ZXDU68 S202 V5.0R02M02 ACB V1.30.01.00 , ZXDU68 S202 V5.0R02M02 ACB V1.30.01.01, ZXDU68 S202 V5.0R02M02 ACB V1.30.01.02, ZXDU68 S202 V5.0R02M02 ACB V1.30.01.03	https://support.zte.com.cn/zte-iccp-support-webui/bulletin/detail/874505866159002595	none	no	total
CVE-2026-53552	9,6	Goploy	Authorization Bypass Through User-Controlled Key; Incorrect Authorization	In versions 1.17.5 and prior	https://github.com/zhenorz/goploy/security/advisories/GHSA-26rh-24rq-i3vv			
CVE-2026-59111	9,3	eObčanka-Identifikace	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Prior to version 3.6.0	https://info.identita.gov.cz/eop/BezpecnostniOznameni/CVE-2026-59111.aspx	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-2026-82454	9,1	commit abf53d6	Improper Verification of Cryptographic Signature	prior to abf53d650875	https://github.com/omnivore-app/omnivore https://github.com/omnivore-app/omnivore/commit/abf53d650875d3d22a994e28e370a9193ea977a https://github.com/omnivore-app/omnivore/pull/4652 https://www.vulncheck.com/advisories/omnivore-before-android-0.227.0-authentication-bypass-via-apple-sign-in	none	yes	partial
CVE-2026-12894	8,8	the Qute template engine	Improper Neutralization of Special Elements Used in a Template Engine		https://access.redhat.com/security/cve/CVE-2026-12894 https://bugzilla.redhat.com/show_bug.cgi?id=2491319	none	no	total
CVE-2026-19806	8,8	The Support Genix – Helpdesk, AI Chatbot, Knowledge Base & Customer Support Ticketing System plugin for Word-Press	Improper Authentication	up to, and including, 1.4.52	https://plugins.trac.wordpress.org/browser/support-genix-lite/tags/1.4.50/core/secondary_helper.php#L754 https://plugins.trac.wordpress.org/browser/support-genix-lite/tags/1.4.50/libs/Apbd_Wps_EncryptionLib.php#L27 https://plugins.trac.wordpress.org/browser/support-genix-lite/tags/1.4.50/models/database/Mapbd_wps_ticket.php#L457 https://plugins.trac.wordpress.org/browser/support-genix-lite/tags/1.4.50/modules/Apbd_wps_settings.php#L152 https://plugins.trac.wordpress.org/browser/support-genix-lite/tags/1.4.50/modules/Apbd_wps_settings.php#L748 https://plugins.trac.wordpress.org/browser/support-genix-lite/tags/1.4.51/core/secondary_helper.php#L754			
CVE-2026-5956	8,8	Site Management Panel	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	through 15062026.	https://siberquvenlik.gov.tr/quvenlik-bildirimleri/detay/tr-26-0955	none	no	total
CVE-2026-81532	8,8	BI Connector ODBC Driver	Stack-based Buffer Overflow	prior to 1.4.10	https://github.com/mongodb/mongo-bi-connector-odbc-driver/releases	none	no	total
CVE-2026-82217	8,8	In Eclipse Theia	Improper Limitation of a Path-name to a Restricted Directory ('Path Traversal')	1.73.0 prior to 1.75.0	https://github.com/eclipse-theia/theia/commit/28da106c254 https://gitlab.eclipse.org/security/vulnerability-reports/-/work_items/624	poc	no	total
CVE-2026-82447	8,8	Skyvern	Improper Neutralization of Special Elements Used in a Template Engine	before 1.0.45	https://github.com/Skyvern-AI/skyvern https://github.com/Skyvern-AI/skyvern/blob/v1.0.44/skyvern/forge/sdk/prompting.py https://github.com/Skyvern-AI/skyvern/blob/v1.0.44/skyvern/forge/sdk/workflow/models/block.py https://github.com/Skyvern-AI/skyvern/commit/d723de621d5b3a340f3cc4d5b46bfe40a9a3124e https://www.vulncheck.com/advisories/skyvern-before-1.0.45-sandbox-escape-via-textpromptblock	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-2026-82882	8,8	Devtron	Missing Authorization	through 2.2.0	https://github.com/devtron-labs/devtron https://github.com/devtron-labs/devtron/blob/v2.2.0/api/apiToken/ApiTokenRestHandler.go https://github.com/devtron-labs/devtron/blob/v2.2.0/pkg/apiToken/ApiTokenService.go https://github.com/devtron-labs/devtron/issues/7013 https://www.vulncheck.com/advisories/devtron-through-2.2.0-missing-authorization-via-webhook-api-token-endpoint			
CVE-2026-82908	8,8	MSI Dragon Center	CWE CATEGORY: Numeric Errors; Integer Overflow or Wraparound	up to 2.0.155.0.	https://drive.google.com/file/d/10o-3GOMAv3tDqQIYWw45rv7MpxYtk/view https://vuldb.com/cve/CVE-2026-82908 https://vuldb.com/submit/877502 https://vuldb.com/vuln/397288 https://vuldb.com/vuln/397288/ctj			
CVE-2026-83497	8,8	the cursor pagination component in the OpenSearch SQL plugin	Deserialization of Untrusted Data	2.8 through 3.6; 2.9 through 3.5	https://aws.amazon.com/security/security-bulletins/2026-092-aws/ https://opensearch.org/artifacts/by-version/#release-2-19-6 https://opensearch.org/artifacts/by-version/#release-3-7-0			
CVE-2026-83596	8,8	WebKitGTK	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')		https://access.redhat.com/security/cve/CVE-2026-83596 https://bugs.webkit.org/show_bug.cgi?id=322969 https://bugzilla.redhat.com/show_bug.cgi?id=2526490			
CVE-2026-82466	8,7	Rodauth	Improper Authentication	before 2.46.0	https://github.com/jeremyevans/rodauth https://github.com/jeremyevans/rodauth/commit/35d74a9f07b2005a8ea75fc11a6539c04f3c2840 https://github.com/jeremyevans/rodauth/security/advisories/GHSA-3pvr-v35r-4r75 https://www.vulncheck.com/advisories/rodauth-before-2.46.0-authentication-bypass-via-webauthn-login	none	no	partial
CVE-2026-55848	8,6	mapfish-print	Improper Restriction of XML External Entity Reference	Prior to 3.28.30, 3.30.32, 3.33.16, 3.31.24,	https://github.com/mapfish/mapfish-print/commit/13beae7a7f970fc3526c1f7ca5db817d8d51fbec https://github.com/mapfish/mapfish-print/commit/23a96e7baa15077bdb0e5fc5a72b18da23af9121 https://github.com/mapfish/mapfish-print/commit/3525e8150fcb5f40095930ccf7aec0d8ce92bbcb https://github.com/mapfish/mapfish-print/commit/56c47d3bf70d8428916dea8ed7005518ad07dc7d https://github.com/mapfish/mapfish-print/commit/a55a24873db5f19b37abac7d59144dc86406c236 https://github.com/mapfish/mapfish-print/commit/d13911ac6e0509444d64e74830f10b14e4dcfd1	poc	yes	partial
CVE-2026-81889	8,6	eFinder; JavaScript using jQuery UI	Server-Side Request Forgery (SSRF)	Prior to 2.1.70	https://github.com/Studio-42/eFinder/commit/191372c1bbebd36fb55af79a84b9984861390ff https://github.com/Studio-42/eFinder/commit/6d997386cd0f1abab4706c220b46b0aea0ecff51 https://github.com/Studio-42/eFinder/releases/tag/2.1.70 https://github.com/Studio-42/eFinder/security/advisories/GHSA-8x3g-jpih-qh5c			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-82641	8,6	keploy	Missing Authentication for Critical Function	versions 3.1.0 through 3.6.25	https://github.com/keploy/keploy https://github.com/keploy/keploy/blob/v3.6.25/pkg/agent/routes/server.go https://github.com/keploy/keploy/commit/a6257d2b3184b85eb30edad345464aa292297b83 https://github.com/keploy/keploy/issues/4394 https://www.vulncheck.com/advisories/keploy-3.1.0-through-3.6.25-unauthenticated-tls-key-exposure	poc	yes	partial
CVE-2026-81287	8,5	Charitable	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	<= 1.8.12.1	https://patchstack.com/database/wordpress/plugin/charitable/vulnerability/wordpress-charitable-plugin-1-8-12-1-sql-injection-vulnerability?_s_id=cve			
CVE-2026-77348	8,2	Wallos	Unintended Proxy or Intermediary ('Confused Deputy'); Server-Side Request Forgery (SSRF); Initialization of a Resource with an Insecure Default	Prior to version 5.0.0	https://github.com/ellite/Wallos/commit/11eaf402e841a628c68a805694227ce66c45f6f3 https://github.com/ellite/Wallos/releases/tag/v5.0.0 https://github.com/ellite/Wallos/security/advisories/GHSA-f8j2-qm83-r2w4 https://github.com/ellite/Wallos/security/advisories/GHSA-hhjq-82f8-m6rc			
CVE-2026-66047	8,1	ProfilePress (wp-user-avatar) WordPress plugin	Missing Authentication for Critical Function; Use of Insufficiently Random Values	before 4.17.2	https://profilepress.com/changelog/ https://wordpress.org/plugins/wp-user-avatar/ https://www.vulncheck.com/advisories/profilepress-wordpress-plugin-unauthenticated-arbitrary-plugin-installation-rce			
CVE-2026-82461	8,1	pac4j-oidc	Improper Verification of Cryptographic Signature	before 6.5.6	https://github.com/pac4j/pac4j https://github.com/pac4j/pac4j/blob/pac4j-parent-6.5.5/pac4j-oidc/src/main/java/org/pac4j/oidc/authorization/generator/KeycloakRolesAuthorizationGenerator.java https://github.com/pac4j/pac4j/commit/2270c3ff70e93cc43831e75702acd5135531237e https://www.pac4j.org/blog/security-advisory-pac4j-core-oidc-saml.html https://www.vulncheck.com/advisories/pac4j-oidc-before-6.5.6-privilege-escalation-via-unverified-keycloak-access-token	none	no	partial
CVE-2026-82475	8,1	iFlytek astron-agent	Missing Authorization	through 1.1.1	https://github.com/iflytek/astron-agent https://github.com/iflytek/astron-agent/blob/v1.1.1/console/backend/toolkit/src/main/java/com/iflytek/astron/console/toolkit/service/workflow/WorkflowService.java https://github.com/iflytek/astron-agent/issues/1590 https://www.vulncheck.com/advisories/iflytek-astron-agent-through-1.1.1-workflow-hijacking-via-missing-ownership-check	poc	no	total
CVE-2026-82636	7,9	Qubes OS	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	prior to qubes-core-dom0-linux 4.3.22	https://news.vcbinator.com/item?id=49496918 https://www.qubes-os.org/news/2026/08/29/qsb-118/	none	no	total
CVE-2026-13732	7,8	GDB's STABS debug format parser	Out-of-bounds Write		https://access.redhat.com/security/cve/CVE-2026-13732 https://bugzilla.redhat.com/show_bug.cgi?id=2494416			
CVE-2026-19702	7,8	Pardus Boot Repair	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	1.0; before 1.0.8.	https://siberquvenlik.gov.tr/quvenlik-bildirimleri/detay/tr-26-0956	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-2026-82457	7,8	su-exec	Incorrect Conversion between Numeric Types	through 0.3	https://gist.github.com/thesmartshadow/ed96e2a88643c34a247c9b7cf9e311be https://github.com/hcopa/su-exec https://github.com/hcopa/su-exec/blob/89c016e6e08749d583efdeda04b9f73e1218e253/su-exec.c https://www.vulncheck.com/advisories/su-exec-through-0.3-privilege-escalation-via-numeric-user-id	poc	no	total
CVE-2026-82474	7,8	Sudo	Protection Mechanism Failure	through 1.9.17p2	https://github.com/sudo-project/sudo https://github.com/sudo-project/sudo/blob/v1.9.17p2/src/exec_pttrace.c https://github.com/sudo-project/sudo/commit/71f8e42cd5a1c8f799540583a2dfb2ae6221edf https://www.vulncheck.com/advisories/sudo-through-1.9-17p2-intercept-policy-bypass-via-execveat			
CVE-2026-41012	7,7	BOSH Director vCenter CPI	Improper Certificate Validation	prior to 98.0.6	https://www.cloudfoundry.org/blog/cve-2026-41012-bosh-vsphere-cpi-improper-cert-validation/	none	no	total
CVE-2026-81490	7,7	a namespace that MongoDB Connector for BI samples	NULL Pointer Dereference	prior to 2.14.31	https://www.mongodb.com/docs/bi-connector/current/release-notes/	none	no	partial
CVE-2026-82869	7,7	ToolJet Database versions	Authorization Bypass Through User-Controlled Key	versions before v3.16.44	https://github.com/ToolJet/ToolJet/security/advisories/GHSA-7vi5-wxlm-qmfg https://www.vulncheck.com/advisories/tooljet-database-before-3.16.44-privilege-escalation-via-jointables	none	no	partial
CVE-2026-40463	7,6	WaveSuite; the CPB Log Files feature	Improper Access Control	25.6; 24.12; 24.6; 23.6	https://www.nokia.com/we-are-nokia/security/product-security-advisory/cve-2026-40463/	none	no	partial
CVE-2026-82017	7,6	IGEL OS	Insufficient Verification of Data Authenticity	before 12.7.6; before 11.11.150	https://blog.amberwolf.com/blog/2026/august/thin-client-thin-crypto-overview/ https://github.com/AmberWolfCyber/DEFCON34-ThinClientThinCrypto/blob/main/scripts/igel/inject_boot_req.py https://kb.igel.com/en/security-safety/current/isn-2026-19-code-execution-via-boot-registry https://media.defcon.org/DEF%20CON%2034/DEF%20CON%2034%20presentations/DEF%20CON%2034%20%20presentations/DEF%20CON%2034%20-%20Darren%20McDonald%20-%20Thin%20Client%20Thin%20Crypto%20-%20Bypassing%20Full-Desk%20Encryption%20Across%20Three%20Major%20Thin%20Clients%20Vendors%20without%20Breaking%20a%20Ci.pdf https://www.vulncheck.com/advisories/igel-os-12-11-boot-registry-parameter-injection-via-unsigned-configuration-area	poc	no	total
CVE-2026-17615	7,5	RESTEasy's SourceProvider	Improper Restriction of XML External Entity Reference		https://access.redhat.com/security/cve/CVE-2026-17615 https://bugzilla.redhat.com/show_bug.cgi?id=2507635	none	yes	partial
CVE-2026-19616	7,5	TBC Technology Inc	Missing Authorization	before v2.2.2.	https://siberquvenlik.gov.tr/quvenlik-bildirimleri/detay/tr-26-0957	none	yes	partial
CVE-2026-19873	7,5	HTML::FormFu versions	Allocation of Resources Without Limits or Throttling; Improper Validation of Specified Quantity in Input	through 2.08	https://github.com/FormFu/HTML-FormFu/issues/71 https://security.metacpan.org/patches/H/HTML-FormFu/2.08/CVE-2026-19873-r1_patch http://www.openwall.com/lists/oss-security/2026/08/31/7	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-2026-19952	7,5	The Frontend Admin by DynamiApps plugin for WordPress	Improper Limitation of a Path-name to a Restricted Directory ('Path Traversal')	up to, and including, 3.29.12.	https://plugins.trac.wordpress.org/browser/acf-frontend-form-element/tags/3.29.10/main/frontend/fields/general/class-upload-file.php#L1014 https://plugins.trac.wordpress.org/browser/acf-frontend-form-element/tags/3.29.10/main/frontend/fields/general/class-upload-file.php#L1044 https://plugins.trac.wordpress.org/browser/acf-frontend-form-element/tags/3.29.10/main/frontend/fields/general/class-upload-file.php#L1047 https://plugins.trac.wordpress.org/browser/acf-frontend-form-element/tags/3.29.10/main/frontend/forms/classes/shortcodes.php#L99 https://plugins.trac.wordpress.org/browser/acf-frontend-form-element/tags/3.29.10/main/frontend/forms/classes/submit.php#L125 https://plugins.trac.wordpress.org/browser/acf-frontend-form-element/tags/3.29.10/main/frontend/forms/classes/submit.php#L276			
CVE-2026-55841	7,5	Graylog	Improper Neutralization of Special Elements	< 6.3.12; >= 7.0.0-alpha.1, < 7.0.7; >= 7.1.0-alpha.1, < 7.1.2	https://github.com/Graylog2/graylog2-server/commit/793df6e8202ea55c15a762e47a2a8a775961dd3f https://github.com/Graylog2/graylog2-server/commit/85dc699d6319aea433583dc239077a3a799c8627 https://github.com/Graylog2/graylog2-server/commit/d5051e604c962ef3d4e5e8e434d0ff4907d2140d https://github.com/Graylog2/graylog2-server/commit/dde76d7432c469887d9a95c208083c5f0f73c70d https://github.com/Graylog2/graylog2-server/pull/26050 https://github.com/Graylog2/graylog2-server/pull/26056	none	yes	partial
CVE-2026-56718	7,5	AJCloud AJY IPC firmware	Improper Limitation of a Path-name to a Restricted Directory ('Path Traversal')	prior to version 01.10715.11.37	https://www.ajcloud.net/ https://www.vulncheck.com/advisories/ajcloud-aiy-ipc-firmware-path-traversal-via-idbhttpd			
CVE-2026-75133	7,5	Keep Backup Daily plugin for WordPress	Missing Authentication for Critical Function	before 2.1.4	https://wordpress.org/plugins/keep-backup-daily/#developers https://www.vulncheck.com/advisories/keep-backup-daily-wordpress-plugin-sensitive-information-exposure-via-kbd-cron-process	none	yes	partial
CVE-2026-76763	7,5	SmallRye GraphQL	Improper Validation of Specified Quantity in Input		https://access.redhat.com/security/cve/CVE-2026-76763 https://bugzilla.redhat.com/show_bug.cgi?id=2519767	none	yes	partial
CVE-2026-77037	7,5	multer; Node	Uncontrolled Resource Consumption; Incomplete Cleanup	2.2.0 prior to 2.3.0	https://cna.openjsf.org/security-advisories.html https://github.com/expressjs/multer/security/advisories/GHSA-gfvm-cv95-igif	none	yes	partial
CVE-2026-81296	7,5	Fluent Forms Pro Add On Pack	Missing Authorization	<= 6.2.12	https://patchstack.com/database/wordpress/plugin/fluentformspro/vulnerability/wordpress-fluent-forms-pro-add-on-pack-plugin-6-2-12-broken-access-control-vulnerability?_s_id=cve			
CVE-2026-81624	7,5	Undertow; JBoss EAP and WildFly	Allocation of Resources Without Limits or Throttling		https://access.redhat.com/security/cve/CVE-2026-81624 https://bugzilla.redhat.com/show_bug.cgi?id=2524868			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-82393	7,5	pnpm	Improper Limitation of a Path-name to a Restricted Directory ('Path Traversal'); External Control of File Name or Path; Improper Control of Generation of Code ('Code Injection')	Prior to 10.34.5 and 11.11.0	https://github.com/pnpm/pnpm/commit/51300fd41c5e4c847635108e373cc3d1f324fa7 https://github.com/pnpm/pnpm/commit/78e29fe5583a1e5d69ea05e414eff310f78d5ed9 https://github.com/pnpm/pnpm/pull/12872 https://github.com/pnpm/pnpm/pull/12890 https://github.com/pnpm/pnpm/releases/tag/v10.34.5 https://github.com/pnpm/pnpm/releases/tag/v11.11.0			
CVE-2026-82397	7,5	Tornado	Uncontrolled Resource Consumption; Improper Validation of Specified Quantity in Input	Prior to 6.5.8	https://github.com/tornadoweb/tornado/commit/8d6363ed7b69d5f0da806efe34d256627a2191de https://github.com/tornadoweb/tornado/pull/3704 https://github.com/tornadoweb/tornado/releases/tag/v6.5.8 https://github.com/tornadoweb/tornado/security/advisories/GHSA-mpf4-983q-p7j4			
CVE-2026-82453	7,5	cleartext without hashing in the user model	Plaintext Storage of a Password	5df942ab6bc46a3bf83dbee8c7970554f92c972d and earlier	https://github.com/iot-ecology/rust-iot-platform/blob/5df942ab6bc46a3bf83dbee8c7970554f92c972d/api/src/biz/user_biz.rs https://www.vulncheck.com/advisories/rust-iot-platform-clear-text-password-storage-via-user-model	none	yes	partial
CVE-2026-82472	7,5	Documenso	Missing Authentication for Critical Function	before 2.13.0	https://github.com/documenso/documenso/blob/v2.12.0/apps/remix/server/api/files/files.ts https://github.com/documenso/documenso/commit/4f346d3c2d5264f221e4d787e162f16051e44114 https://www.vulncheck.com/advisories/documenso-before-2.13.0-unauthenticated-file-upload-via-api-files-upload-pdf	none	yes	partial
CVE-2026-82639	7,5	NextChat	Improper Input Validation	from 2.15.8 through 2.16.1	https://github.com/ChatGPTNextWeb/NextChat/blob/v2.16.1/app/api/proxy.ts https://github.com/ChatGPTNextWeb/NextChat/issues/6814 https://www.vulncheck.com/advisories/nextchat-2.15.8-through-2.16.1-openai-api-key-disclosure	poc	yes	partial
CVE-2026-82225	7,4	RegistrationMagic	Authentication Bypass Using an Alternate Path or Channel	<= 6.0.9.8	https://patchstack.com/database/wordpress/plugin/custom-registration-form-builder-with-submission-manager/vulnerability/wordpress-registrationmagic-plugin-6-0-9-8-broken-authentication-vulnerability?_s_id=cve			
CVE-2026-82801	7,3	NASA earthdata-search	Server-Side Request Forgery (SSRF)	1.0.0	https://github.com/natanmorette/thoropass/thoropass-vuln-research-program/tree/main/2026/Unauthenticated%20Scale%20Image%20SSRF https://vuln.db.com/cve/CVE-2026-82801 https://vuln.db.com/submit/881731 https://vuln.db.com/vuln/397222 https://vuln.db.com/vuln/397222/ctj	poc	yes	partial
CVE-2026-82815	7,3	MegaEase EaseProbe	Incorrect Privilege Assignment; Improper Access Control	up to 2.3.0.	https://github.com/BiBi8BoBo/megaease_easeprobe-unvalidated-X-Forwarded-For-header https://vuln.db.com/cve/CVE-2026-82815 https://vuln.db.com/submit/875371 https://vuln.db.com/vuln/397232 https://vuln.db.com/vuln/397232/ctj	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-2026-82914	7,3	kishan0725 Hospital-Management-System	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'); Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://uvxbywu62gm.feishu.cn/wiki/NKztwPKs3i07urk5hARcG6venZ7?from=from_copylink https://vuldb.com/cve/CVE-2026-82914 https://vuldb.com/submit/878520 https://vuldb.com/vuln/397291 https://vuldb.com/vuln/397291/cti			
CVE-2026-82919	7,3	cu silicon	Improper Authentication; Missing Authentication for Critical Function	up to 0.1.5.	https://vuldb.com/cve/CVE-2026-82919 https://vuldb.com/submit/879029 https://vuldb.com/vuln/397299 https://vuldb.com/vuln/397299/cti	none	yes	partial
CVE-2026-82921	7,3	ShopEx ECShop	Improper Access Control; Unrestricted Upload of File with Dangerous Type	up to 2.5.1.	https://uvxbywu62gm.feishu.cn/wiki/TNENwNliltivqtk2uABci02Indc?from=from_copylink https://vuldb.com/cve/CVE-2026-82921 https://vuldb.com/submit/879229 https://vuldb.com/vuln/397301 https://vuldb.com/vuln/397301/cti			
CVE-2026-82957	7,3	hyperledger-firefly firefly	Server-Side Request Forgery (SSRF)	up to 1.4.0.	https://vuldb.com/cve/CVE-2026-82957 https://vuldb.com/submit/879847 https://vuldb.com/vuln/397306 https://vuldb.com/vuln/397306/cti			
CVE-2026-19573	7,2	The Affiliate Super Assistant plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 1.10.2	https://plugins.trac.wordpress.org/browser/amazonsimpleadmin/tags/1.9.0/AsaCore.php#L3296 https://plugins.trac.wordpress.org/browser/amazonsimpleadmin/tags/1.9.0/AsaCore.php#L3301 https://plugins.trac.wordpress.org/browser/amazonsimpleadmin/tags/1.9.0/AsaCore.php#L4043 https://plugins.trac.wordpress.org/browser/amazonsimpleadmin/tags/1.9.0/AsaCore.php#L4137 https://plugins.trac.wordpress.org/changeset/3672410/amazonsimpleadmin https://www.wordfence.com/threat-intel/vulnerabilities/id/9e6abc4e-7f21-47ac-95ff-b6d997c70e23?source=cve			
CVE-2026-19796	7,2	The Listdom: AI-powered Business Directory with Classifieds Ads Listings plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 5.8.1	https://plugins.trac.wordpress.org/browser/listdom/tags/5.8.1/app/includes/entity/listing.php#L196 https://plugins.trac.wordpress.org/browser/listdom/tags/5.8.1/app/includes/ptypes/listing/single.php#L560 https://plugins.trac.wordpress.org/browser/listdom/tags/5.8.1/app/includes/ptypes/listing/single.php#L82 https://plugins.trac.wordpress.org/browser/listdom/tags/5.8.1/app/includes/shortcodes/dashboard.php#L739 https://plugins.trac.wordpress.org/changeset?reponame=&old=3661300%40listdom&new=3661300%40listdom https://www.wordfence.com/threat-intel/vulnerabilities/id/0d36650d-6997-457d-ac8d-04f98e2080ef?source=cve			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-75921	7,2	Master Addons for Elementor – Elementor Addons, Widgets, Mega Menu Builder, Popup Builder, Widget Builder & Template Kits	Incorrect Authorization	up to, and including, 3.1.9	https://plugins.trac.wordpress.org/browser/master-addons/tags/3.1.8/inc/admin/page-importer.php#L84 https://plugins.trac.wordpress.org/browser/master-addons/tags/3.1.8/inc/admin/templates/kits/class-importer.php#L2124 https://plugins.trac.wordpress.org/browser/master-addons/tags/3.1.8/inc/admin/templates/kits/class-importer.php#L2198 https://plugins.trac.wordpress.org/browser/master-addons/tags/3.1.8/inc/admin/templates/kits/class-importer.php#L49 https://plugins.trac.wordpress.org/browser/master-addons/tags/3.1.9/inc/admin/page-importer.php#L84 https://plugins.trac.wordpress.org/browser/master-addons/tags/3.1.9/inc/admin/templates/kits/class-importer.php#L2124			

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 Two Known Exploited Vulnerabilities to Catalog CISA	▪ CVE-2026-81578 PaperCut NG/MF Missing Authentication for Critical Function Vulnerability ▪ CVE-2026-82078 PaperCut NG/MF Unsafe Reflection Vulnerability	https://cisa.gov/news-events/alerts/2026/08/31/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
Hackers Target AWS Root Accounts at 150+ Organizations in Password-Spraying Campaign	https://cybersecuritynews.com/hackers-target-aws-root-accounts
PaperCut Exploitation Escalates to Active Intrusions	https://securityweek.com/papercut-exploitation-escalates-to-active-intrusions
Anthropic Hardens Claude Security After AI Models Gain Unauthorized Access to Real Systems	https://cybersecuritynews.com/anthropic-hardens-claude-security
BGP Hijack Diverts Softaculous Traffic to Deliver Malicious Virtualizer Update	https://cybersecuritynews.com/virtualizer-compromise
Cronos blockchain restarts after \$74 million Tectonic exploit	https://bleepingcomputer.com/news/security/cronos-blockchain-restarts-after-74-million-tectonic-exploit

Microsoft warns of TerminalFix attacks deploying reverse tunnels	https://bleepingcomputer.com/news/security/microsoft-warns-of-terminalfix-attacks-deploying-reverse-tunnels
Microsoft Exchange Online outage causes email failures, auth issues	https://bleepingcomputer.com/news/microsoft/microsoft-exchange-online-outage-causes-email-failures-auth-issues
OpenAI confirms ChatGPT outage as users report errors	https://bleepingcomputer.com/news/artificial-intelligence/openai-confirms-chatgpt-outage-as-users-report-errors
Broadcom Launches VMware AI Factory to Secure Enterprise AI Agents	https://cybersecuritynews.com/broadcom-vmware-ai-factory
Microsoft Investigating New Exchange Online Outage Tracked as EX1464935 [Updated]	https://cybersecuritynews.com/microsoft-new-exchange-online
Chinese Fire Ant hackers turn Cisco routers into spying platforms	https://bleepingcomputer.com/news/security/chinese-fire-ant-hackers-turn-cisco-routers-into-spying-platforms
Security Risk Advisors Launches SCALR AI as a Free SOC AI Platform for Security Teams	https://cybersecuritynews.com/security-risk-advisors-launches-scalr-ai-as-a-free-soc-ai-platform-for-security-teams
Privacy Policy	https://cybersecuritynews.com/privacy-policy-2
🔥 Weekly Recap: Chinese Spy Proxy, AI Agents Go Off-Task, Router Backdoors and More	https://thehackernews.com/2026/08/weekly-recap-chinese-spy-proxy-ai.html
EU Designates ChatGPT as Very Large Online Search Engine After Crossing 45 Million Users	https://cybersecuritynews.com/eu-designates-chatgpt
Brave Unveils New Email Aliases to Keep Your Personal Email Address Private	https://cybersecuritynews.com/brave-unveils-new-email-aliases
What the Hugging Face Incident Teaches Security Leaders About AI Agent Access	https://securityweek.com/what-the-hugging-face-incident-teaches-security-leaders-about-ai-agent-access
Boston Scientific Still Recovering From Cyberattack	https://securityweek.com/boston-scientific-still-recovering-from-cyberattack
Microsoft says Windows 11 KB5120998 update resets mouse settings	https://bleepingcomputer.com/news/security/microsoft-says-windows-11-kb5120998-update-resets-mouse-settings
Nigerians extradited to US for sextortion, deaths of two teens	https://bleepingcomputer.com/news/security/nigerians-charged-US-over-sextortion-deaths-of-us-teens

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
McKesson Confirms Data Breach as Attacker Deadline Looms	https://securityweek.com/mckesson-confirms-data-breach-as-attacker-deadline-looms
Extortion Group Claims Manchester Airports Group Data Breach	https://securityweek.com/extortion-group-claims-manchester-airports-group-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
CISA Warns of Multiple PaperCut NG/MF Vulnerabilities Actively Exploited in Attacks	https://cybersecuritynews.com/papercut-ng-mf-vulnerabilities-exploited
D-Link Router Flaws Let Unauthenticated Attackers Change Admin Password and Steal Wi-Fi Credentials	https://cybersecuritynews.com/d-link-router-flaws
HardBreacher PoC Claims Kaspersky Endpoint 0-Day Privilege Escalation on Windows 11	https://cybersecuritynews.com/hardbreacher-kaspersky-zero-day
Nightmare Eclipse Drops 'HardBreacher' Kaspersky Product Exploit	https://securityweek.com/nightmare-eclipse-drops-hardbreacher-kaspersky-product-exploit
Critical Ruby on Rails Vulnerability in Attackers' Crosshairs	https://securityweek.com/critical-ruby-on-rails-vulnerability-in-attackers-crosshairs
Composer Flaw Lets Malicious Dependencies Expose SSH Keys and Sensitive Files	https://cybersecuritynews.com/composer-flaw-expose-ssh-keys
Critical Microsoft Flaw Lets Hackers Remotely Control Android Devices Without a Login	https://cybersecuritynews.com/microsoft-flaw
More Details Emerge on Exploited PaperCut Vulnerabilities	https://securityweek.com/more-details-emerge-on-exploited-papercut-vulnerabilities
Five Critical WordPress Plugin and Theme Flaws Enable Site Takeover or RCE	https://thehackernews.com/2026/08/five-critical-wordpress-plugin-and.html
Critical ServiceNow Flaws Let Attackers Execute Code and Access Data	https://cybersecuritynews.com/servicenow-fixes-critical-flaws

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
ServiceNow Patches 3 Critical Code Injection Vulnerabilities	https://securityweek.com/servicenow-patches-3-critical-code-injection-vulnerabilities

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
Anthropic Users Hit by Infostealer Attacks, Session Thefts	https://darkreading.com/cyberattacks-data-breaches/anthropic-users-infostealer-attacks-session-thefts
Hackers Hide ValleyRAT Backdoor Inside Adware Targeting Users in China and India	https://cybersecuritynews.com/hackers-hide-valleyrat-backdoor
Berlin confirms data theft after Rhysida ransomware attack claims	https://bleepingcomputer.com/news/security/berlin-confirms-data-theft-after-rhysida-ransomware-attack-claims
Anthropic Warns Claude Users of Infostealer Malware Infections	https://securityweek.com/anthropic-warns-claude-users-of-infostealer-malware-infections
Popular npm Package With 150K+ Weekly Downloads Hit by Credential-Stealing Supply-Chain Worm	https://cybersecuritynews.com/popular-npm-package
New AI-Built Malware Watches How Security Teams Remove It and Fights Back	https://cybersecuritynews.com/new-ai-built-malware-watches
Hackers' Own Malware Infection Exposes Their RATs, Phishing Kits and Attack Infrastructure	https://cybersecuritynews.com/hackers-own-malware-infection
Free Router DNS Tweak Blocks Malware and Phishing Across Home Networks	https://cybersecuritynews.com/router-dns-tweak-blocks-malware
Hackers Steal Claude Login Sessions With Infostealer Malware to Hijack Accounts	https://cybersecuritynews.com/hackers-steal-claude-login-sessions
Anthropic warns infostealer malware is hijacking Claude sessions to drain usage	https://bleepingcomputer.com/news/artificial-intelligence/anthropic-warns-infostealer-malware-is-hijacking-claude-sessions-to-drain-usage
Malvertising Is Moving From Deceptive Content to Weaponized Infrastructure	https://cybersecuritynews.com/malvertising-is-moving-from-deceptive-content-to-weaponized-infrastructure

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
-	-

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 29/08/2026–01/09/2026, 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/