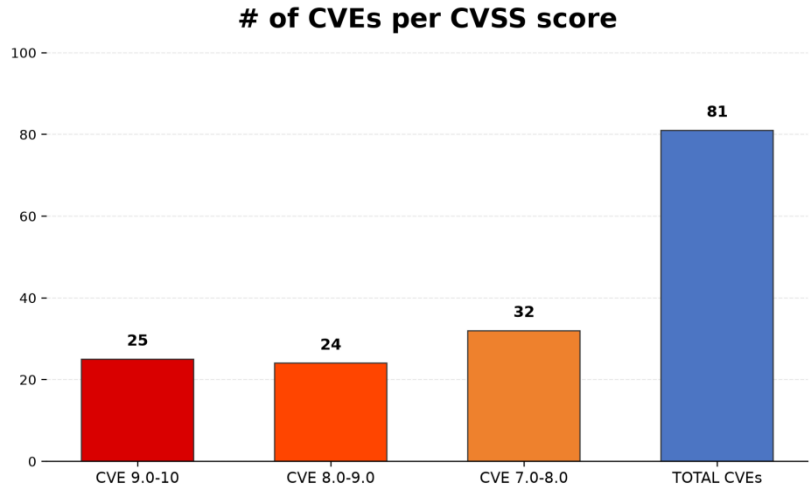
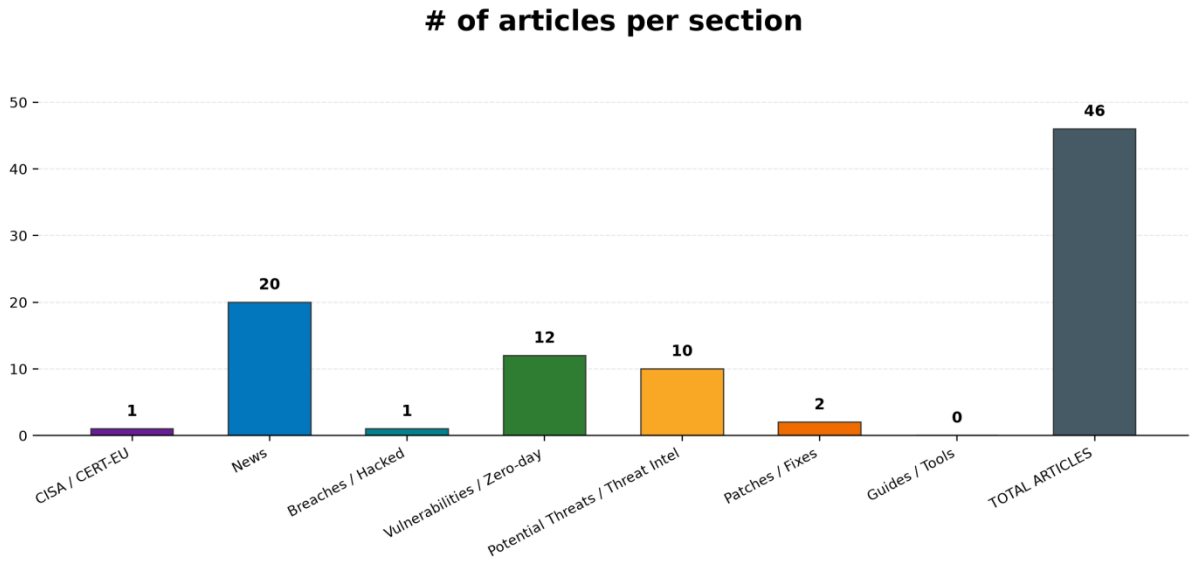
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 22/08/2026 - 25/08/2026





Contents

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-2026-74612	10,0	Linux		718a18a0c8a67f97781e40bdef7cdd055c430996 prior to 0c3024afabb8064b141f3cedcb1ddd6ab05ad9d5; 718a18a0c8a67f97781e40bdef7cdd055c430996 prior to 2f2a7f3f8b9f1bffc9b0488aa02b6951b2aec139; 718a18a0c8a67f97781e40bdef7cdd055c430996 prior to 41b96667d42b74bb4b137f1bb78b611a953c5943; 718a18a0c8a67f97781e40bdef7cdd055c430996 prior to cdf745b7a777f87f51666e5d8f4c6fc279bcf54d; 718a18a0c8a67f97781e40bdef7cdd055c430996 prior to 3205b0652a37255dbb7ca8f3d942c8d8aa677c21; 718a18a0c8a67f97781e40bdef7cdd055c430996 prior to cb6379fe-aaff11c4e1e79c26c745ffa23182768a; 5.18	https://git.kernel.org/stable/c/0c3024afabb8064b141f3cedcb1ddd6ab05ad9d5 https://git.kernel.org/stable/c/2f2a7f3f8b9f1bffc9b0488aa02b6951b2aec139 https://git.kernel.org/stable/c/3205b0652a37255dbb7ca8f3d942c8d8aa677c21 https://git.kernel.org/stable/c/41b96667d42b74bb4b137f1bb78b611a953c5943 https://git.kernel.org/stable/c/cb6379fe-aaff11c4e1e79c26c745ffa23182768a https://git.kernel.org/stable/c/cdf745b7a777f87f51666e5d8f4c6fc279bcf54d			
CVE-2026-32559	9,9	UltimateAI	Unrestricted Upload of File with Dangerous Type	<= 3.1.0	https://patchstack.com/database/wordpress/plugin/ultimate_ai/vulnerability/wordpress-ultimateai-plugin-3-1-0-arbitrary-file-upload-vulnerability?_s_id=cve			
CVE-2026-66897	9,9	LXD's instance template	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'); Relative Path Traversal	4.0.0 prior to 4.0.13; 5.0.0 prior to 5.0.9; 5.21.0 prior to 5.21.7; 6.0 prior to 6.10	https://github.com/canonical/lxd/security/advisories/GHSA-q39m-8fx9-42fv	none	no	total
CVE-2026-78155	9,9	StackGres operator	Untrusted Search Path	1.18.8 and earlier	https://gitlab.com/ongresinc/stackgres/-/work_items/3177	none	no	total
CVE-2026-13214	9,8	The OCPP	Out-of-bounds Write	4.3.0 prior to 4.4.2	https://github.com/zephyrproject-rtos/zephyr/commit/afbf880b04188ae53451a0ade4ac62b654fdff34 https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-fghf-6v24-4px2			
CVE-2026-32563	9,8	ACPT (Pro) - Custom Post Types Plugin for WordPress	Deserialization of Untrusted Data	<= 2.0.63	https://patchstack.com/database/wordpress/plugin/advanced-custom-post-type/vulnerability/wordpress-acpt-pro-custom-post-types-plugin-for-wordpress-plugin-2-0-63-php-object-injection-vulnerability?_s_id=cve			
CVE-2026-56705	9,8	Adminer	External Control of File Name or Path	before 5.4.3	https://github.com/vrana/adminer/security/advisories/GHSA-r4x9-5m63-3vxw https://www.vulncheck.com/advisories/adminer-before-remote-code-execution-via-mssql-pdo-dsn-injection			
CVE-2026-56710	9,8	Grav Login plugin versions	Incorrect Authorization	versions before 1.0.16	https://github.com/getgrav/grav/security/advisories/GHSA-985r-mpj8-5rgw https://www.vulncheck.com/advisories/grav-login-plugin-before-privilege-escalation-via-unlock			
CVE-2026-71914	9,8	Multiple DrayTek VigorAP models; the dray_apm component	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	prior to 1.4.11; prior to 1.4.12; prior to 1.4.13; prior to 1.4.15; prior to 1.4.22	https://www.draytek.com/about/security-advisory/multiple-remote-code-execution-and-buffer-overflow-vulnerabilities-in-vigorap-series-august-2026/ https://www.vulncheck.com/advisories/draytek-vigorap-multiple-models-pre-authentication-os-command-injection-via-dray-apm	none	yes	total

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-71921	9,8	Multiple DrayTek VigorSwitch models; the setget	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	prior to 3.9.10; prior to 2.10.6; prior to 2.10.7; prior to 3.10.6; prior to 2.9.10	https://www.draytek.com/about/security-advisory/multiple-vulnerabilities-in-vigorswitch-series-august-2026/ https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-pre-authentication-os-command-injection-via-setget-cgi			
CVE-2026-74588	9,8	sctp: keep chunk->transport in step with the list it is queued on		1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to 6575fb17230814b48b471727c8410c0aadff9274; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to 6b9e2ea2057113f3393990ba646d2d97c719a80d; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to 874a7c2b5e184f06134fdfde27e9ce9271bafe58; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to 1adf929121e13e0b19200bb9fef715b918d483fe; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to e2e7c1de0e226ca1b7fea2de57a6c9bca408709b; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to 2b3b5eec8b2c30ee237e3c31a6a38de9c39d804d; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to 5ccf35ef0ed6059cdf8b1f4606a6584d5b67166b; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to 9f2cf069a9a72a2d6b97ca8b4c70e714aac99749; 2.6.12	https://git.kernel.org/stable/c/1adf929121e13e0b19200bb9fef715b918d483fe https://git.kernel.org/stable/c/2b3b5eec8b2c30ee237e3c31a6a38de9c39d804d https://git.kernel.org/stable/c/5ccf35ef0ed6059cdf8b1f4606a6584d5b67166b https://git.kernel.org/stable/c/6575fb17230814b48b471727c8410c0aadff9274 https://git.kernel.org/stable/c/6b9e2ea2057113f3393990ba646d2d97c719a80d https://git.kernel.org/stable/c/874a7c2b5e184f06134fdfde27e9ce9271bafe58			
CVE-2026-74608	9,8	cifs_try_adding_channels() cifs_try_adding_channels() takes a temporary reference to an interface		cbc53148cc0946b72d62a3c53870cb22ce4ec284 prior to 64d7584e62ac8cdc750455c5fdc6008fc2de4f06; cff97d683a083b862a8bb24309e0f4d2d928128a prior to c292d4686f717c03e5022fc4ae7c782f39a94915; 6aac002bcfd554aff6d3ebb55e1660d078d70ab0 prior to 47dfac48bce7198ad4f1a388fc8c9491f878ac3b; 6aac002bcfd554aff6d3ebb55e1660d078d70ab0 prior to 1ffac-badc14530e55b8d86f7b917524f6a0fb891; 6aac002bcfd554aff6d3ebb55e1660d078d70ab0 prior to 1305eadc6a7d78a8d0a52eee29ddd2d9e8a27805; 6aac002bcfd554aff6d3ebb55e1660d078d70ab0 prior to 4986410316b1ae0e63c6ce418e4eb196723626e7; 22a6c5b3425f327e7f4c3606a72277dce82c7d83; 6.1.78 prior to 6.1.183; 6.6.17 prior to 6.6.152; 6.7.5 prior to 6.8; 6.8	https://git.kernel.org/stable/c/1305eadc6a7d78a8d0a52eee29ddd2d9e8a27805 https://git.kernel.org/stable/c/1ffac-badc14530e55b8d86f7b917524f6a0fb891 https://git.kernel.org/stable/c/47dfac48bce7198ad4f1a388fc8c9491f878ac3b https://git.kernel.org/stable/c/4986410316b1ae0e63c6ce418e4eb196723626e7 https://git.kernel.org/stable/c/64d7584e62ac8cdc750455c5fdc6008fc2de4f06 https://git.kernel.org/stable/c/c292d4686f717c03e5022fc4ae7c782f39a94915			
CVE-2026-74617	9,8	dibs_dev_alloc() dibs->lock		cc21191b584c6f7836b0f10774f8278b7cbfba10 prior to fe79571f40434b257d68cbfb7b3ae93a794d8a11; cc21191b584c6f7836b0f10774f8278b7cbfba10 prior to 2926031acba100d0c18fcfaa7a2ed29609318848; cc21191b584c6f7836b0f10774f8278b7cbfba10 prior to c27e360545373b7aee9862a5beef3b9fb3df0c25; 6.18	https://git.kernel.org/stable/c/2926031acba100d0c18fcfaa7a2ed29609318848 https://git.kernel.org/stable/c/c27e360545373b7aee9862a5beef3b9fb3df0c25 https://git.kernel.org/stable/c/fe79571f40434b257d68cbfb7b3ae93a794d8a11			
CVE-2026-76904	9,8	GeoTools	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	in version 30.5 and prior	https://github.com/geotools/geotools/commit/d821c4d321dd91c22e31fcd5b1ce676645da5176 https://github.com/geotools/geotools/pull/5829 https://github.com/geotools/geotools/releases/tag/33.6 https://github.com/geotools/geotools/releases/tag/34.5 https://github.com/geotools/geotools/releases/tag/35.1 https://github.com/geotools/geotools/security/advisories/GHSA-mqjf-5f49-2fjh	none	yes	total

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-77000	9,8	The WP Social Media Login WordPress plugin	Improper Authentication	through 1.0.6	https://wpscan.com/vulnerability/3051dece-7ecb-4911-bf13-291ebdc34bff/	none	yes	total
CVE-2026-77001	9,8	The Social Login & Sharing buttons with Analytics By So-Clever WordPress plugin	Improper Authentication	through 1.2.0	https://wpscan.com/vulnerability/01c78c78-3915-44da-824a-f68074985c75/	none	yes	total
CVE-2026-77002	9,8	The SmilePass Selfie Login WordPress plugin	Improper Authentication	through 1.0.2	https://wpscan.com/vulnerability/51236907-a1b4-4c3b-8c39-adafcab7a2ef/	none	yes	total
CVE-2026-77915	9,8	rConfig	Missing Authentication for Critical Function; Initialization of a Resource with an Insecure Default	before 8.2.13	https://github.com/rconfig/rconfig/releases#release-core-8.2.10 https://github.com/rconfig/rconfig/security/advisories/GHSA-w3hx-9cxq-5ccr https://www.vulncheck.com/advisories/rconfig-unauthorized-admin-registration-via-web-php			
CVE-2026-78262	9,8	WP Project Manager	Deserialization of Untrusted Data	<= 4.0.6	https://patchstack.com/database/wordpress/plugin/wedevs-project-manager/vulnerability/wordpress-wp-project-manager-plugin-4-0-6-php-object-injection-vulnerability?_s_id=cve			
CVE-2026-78265	9,8	The Events Calendar	Deserialization of Untrusted Data	<= 6.17.2	https://patchstack.com/database/wordpress/plugin/the-events-calendar/vulnerability/wordpress-the-events-calendar-plugin-6-17-2-php-object-injection-vulnerability?_s_id=cve			
CVE-2026-78267	9,8	TranslatePress	Incorrect Privilege Assignment	<= 3.3.2	https://patchstack.com/database/wordpress/plugin/translatepress-multilingual/vulnerability/wordpress-translatepress-plugin-3-3-2-privilege-escalation-vulnerability?_s_id=cve			
CVE-2026-78477	9,8	The Jawn theme for WordPress; all	Incorrect Privilege Assignment	up to, and including, 1.4.2.	https://patchstack.com/database/wordpress/theme/jawn/vulnerability/wordpress-jawn-theme-1-4-2-privilege-escalation-vulnerability https://www.wordfence.com/threat-intel/vulnerabilities/id/e0642c85-ee01-497c-8dc3-42e3ffc02995?source=cve			
CVE-2026-78676	9,8	GitPython	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	before 3.1.59	https://github.com/gitpython-developers/GitPython/security/advisories/GHSA-284h-m62g-qf8w https://www.vulncheck.com/advisories/gitpython-before-remote-code-execution-via-config-injection			
CVE-2026-76840	9,6	rustdesk	Improper Input Validation; Out-of-bounds Write	1.4.9 and earlier	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-m37j-jcr2-8qcc https://github.com/rustdesk/rustdesk https://github.com/rustdesk/rustdesk/blob/1.4.9/libs/clipboard/src/windows/wf_cliprdr.c https://github.com/rustdesk/rustdesk/pull/15515 https://www.vulncheck.com/advisories/rustdesk-through-heap-buffer-overflow-via-unvalidated-cliprdr-filecontentsresponse-length	none	no	partial
CVE-2026-76835	9,1	oauth2-proxy	Authentication Bypass by Spoofing	7.15.2 through 7.15.4	https://github.com/oauth2-proxy/oauth2-proxy https://github.com/oauth2-proxy/oauth2-proxy/blob/v7.15.4/pkg/apis/middleware/scope.go https://github.com/oauth2-proxy/oauth2-proxy/issues/3506 https://github.com/oauth2-proxy/oauth2-proxy/security/advisories/GHSA-7x63-xv5r-3p2x https://www.vulncheck.com/advisories/oauth2-proxy-through-authentication-bypass-via-x-forwarded-uri-under-the-default-trusted-proxy-set	poc	yes	total
CVE-2026-19200	8,9	The Velociraptor verify() VQL function	Improper Control of Generation of Code ('Code Injection'); Missing Authorization	prior to 0.77.2	http://docs.velociraptor.app/announcements/advisories/cve-2026-19200/ https://github.com/Velocidex/velociraptor/pull/4962	none	no	total
CVE-2026-30864	8,9	Combodo iTop	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Prior to 3.2.3	https://github.com/Combodo/iTop/security/advisories/GHSA-6pqv-3fcp-c5q2	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-2025-36940	8,8	a zircon kernel pager proxy (Fuchsia)	Use After Free	F30.1.1	https://support.google.com/product-documentation/answer/17072818?hl=en&ref_topic=12974021&sjid=10451061435205708316-NC	none	no	total
CVE-2026-13212	8,8	zephyr	Improper Validation of Array Index	4.2.0 prior to 4.4.2	https://github.com/zephyrproject-rtos/zephyr/commit/fe47dbca080957c425383cc1d5bdc7d48a41d4a5 https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-7884-373w-qghx	none	no	total
CVE-2026-32560	8,8	MagicAI for WordPress - AI Text, Image, Chat, Code, and Voice Generator	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')	<= 1.4	https://patchstack.com/database/wordpress/plugin/magicai-wp/vulnerability/wordpress-magicai-for-wordpress-ai-text-image-chat-code-and-voice-generator-plugin-1-4-local-file-inclusion-vulnerability?_s_id=cve			
CVE-2026-32561	8,8	Booking Hub	Incorrect Privilege Assignment	<= 1.3.0	https://patchstack.com/database/wordpress/plugin/booking-hub/vulnerability/wordpress-booking-hub-plugin-1-3-0-privilege-escalation-vulnerability?_s_id=cve			
CVE-2026-56702	8,8	Adminer versions	Unrestricted Upload of File with Dangerous Type	versions before 5.4.3	https://github.com/vrana/adminer/security/advisories/GHSA-vcvj-rwwm-x6g5 https://www.vulncheck.com/advisories/adminer-before-unrestricted-file-upload-via-adminerfileupload			
CVE-2026-59565	8,8	Client Connector	Improper Handling of Values	prior to Windows: 4.6.0.457, 4.7.0.317, 4.8.0.232, 4.9.0.372	https://help.zscaler.com/zscaler-client-connector/client-connector-app-release-summary-2026	none	no	total
CVE-2026-59808	8,8	AVideo	Missing Authentication for Critical Function	9c39d8c8b4c1f75540788d6b391740852ceb0732 and earlier	https://github.com/WWBN/AVideo/security/advisories/GHSA-g32p-rw3g-8x3r https://www.vulncheck.com/advisories/avideo-authentication-bypass-via-unkeyed-video-hash-disclosure	poc	no	total
CVE-2026-62316	8,8	UFO	Exposure of Sensitive Information to an Unauthorized Actor; Origin Validation Error	Prior to 3.0.8	https://github.com/microsoft/UFO/commit/3851c5d4e17c2865c56a94a6530692bf6e7a9b02 https://github.com/microsoft/UFO/releases/tag/v3.0.8 https://github.com/microsoft/UFO/security/advisories/GHSA-vf4c-mf32-gf2h			
CVE-2026-75574	8,8	The Grav Email plugin (getgrav/grav-plugin-email)	Improper Neutralization of Special Elements Used in a Template Engine	before 4.2.2	https://github.com/getgrav/grav/security/advisories/GHSA-gh8j-q67c-j53f https://www.vulncheck.com/advisories/grav-before-remote-code-execution-via-email-twig			
CVE-2026-76073	8,8	label-studio	Authorization Bypass Through User-Controlled Key	1.23.0 and earlier	https://github.com/HumanSignal/label-studio https://github.com/HumanSignal/label-studio/blob/1.23.0/label_studio/tasks/api.py https://github.com/HumanSignal/label-studio/issues/9796 https://www.vulncheck.com/advisories/label-studio-through-cross-organization-annotation-access-via-unscoped-annotationapi-queryset			
CVE-2026-76789	8,8	The Slider Hero with Video Background, Animation WordPress plugin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	before 9.1.3	https://wpscan.com/vulnerability/f9f5485c-6231-492c-b214-8da87a2bf4d1/	none	no	partial
CVE-2026-76836	8,8	AzuraCast	Improper Control of Generation of Code ('Code Injection'); Incorrect Authorization	0.23.8 and earlier	https://github.com/AzuraCast/AzuraCast https://github.com/AzuraCast/AzuraCast/blob/0.23.8/backend/src/Entity/Station.php https://github.com/AzuraCast/AzuraCast/blob/0.23.8/backend/src/Radio/Backend/Liquidsoap/ConfigWriter.php https://github.com/AzuraCast/AzuraCast/security/advisories/GHSA-q8wq-3qq7-8pc7 https://www.vulncheck.com/advisories/azuracast-through-liquidsoap-configuration-write-via-profile-edit-serialization-group-bypass	poc	no	total
CVE-2026-76847	8,8	act starts an HTTP Artifacts V4	Use of Hard-coded Cryptographic Key; Missing Authorization	0.2.81 through 0.2.89	https://github.com/nektos/act https://github.com/nektos/act/blob/v0.2.89/cmd/root.go https://github.com/nektos/act/blob/v0.2.89/pkg/artifacts/artifacts_v4.go https://www.vulncheck.com/advisories/act-through-missing-authorization-in-the-artifacts-v4-backend			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-78314	8,8	Delta DIAEnergie	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.11.00.002 and earlier	https://filecenter.deltaww.com/news/download/doc/Delta-PCSA-2026-00015_DIAEnergie%20SQL%20Injection%20Vulberabilities_v1.0.pdf	none	no	total
CVE-2026-78376	8,8	WebKitGTK	Use After Free		https://access.redhat.com/security/cve/CVE-2026-78376 https://bugzilla.redhat.com/show_bug.cgi?id=2521858 https://github.com/WebKit/WebKit/pull/72142	none	no	total
CVE-2026-78685	8,8	Medical Practice Management System	Improper Verification of Source of a Communication Channel	2.4.2.8 through 2.5.1.9	https://www.twcert.org.tw/en/cp-139-11128-8bd30-2.html https://www.twcert.org.tw/tw/cp-132-11127-cda76-1.html			
CVE-2026-78284	8,6	MasterStudy LMS	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	<= 3.7.42	https://patchstack.com/database/wordpress/plugin/masterstudy-lms-learning-management-system/vulnerability/wordpress-masterstudy-lms-plugin-3-7-42-arbitrary-file-deletion-vulnerability?_s_id=cve			
CVE-2026-10053	8,5	GitLab CE/EE	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18; before 19.0.6, 19.1; before 19.1.4; before 19.2.2	https://gitlab.com/gitlab-org/gitlab/-/work_items/601596 https://hackerone.com/reports/3754194	none	no	total
CVE-2026-76842	8,2	mercadopago	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	3.4.0 and earlier	https://github.com/mercadopago/sdk-nodejs https://github.com/mercadopago/sdk-nodejs/blob/3.4.0/src/clients/payment/get/index.ts https://github.com/mercadopago/sdk-nodejs/pull/451 https://www.vulncheck.com/advisories/mercado-pago-node-js-sdk-through-path-injection-via-unencoded-identifiers-in-payment-clients	none	yes	partial
CVE-2026-18052	8,1	The ManageWP Worker WordPress plugin	Improper Authentication	before 4.9.37	https://wpscan.com/vulnerability/e1e8c313-f7ea-4f3a-85c0-4f33dfe0710d/	none	no	total
CVE-2026-76793	8,1	The Firebase Authentication WordPress plugin	Improper Authentication	before 1.7.1	https://wpscan.com/vulnerability/0414ef2b-0d97-41c7-9146-f31ace8b66b2/	none	no	total
CVE-2026-78414	8,0	the Web Administration interface of Network Optix Nx Witness VMS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	before version 6.1.3; 6.1.3 or later	https://support.networkoptix.com/hc/en-us/articles/42950508518679-Security-Advisory-Cross-Site-Scripting-XSS-in-Merge-with-Another-Site-Dropdown	none	no	total
CVE-2026-16783	7,8	3ds Max	Out-of-bounds Write	2027.0.0 prior to 2027.2.0; 2026.0.0 prior to 2026.3.4	https://www.autodesk.com/products/autodesk-access/overview https://www.autodesk.com/trust/security-advisories/adsk-sa-2026-0014			
CVE-2026-57998	7,8	better-npm-audit	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	through 3.11.0	https://github.com/jeemok/better-npm-audit https://github.com/jeemok/better-npm-audit/blob/fd99a0f41ff4342b8a0a6fdbe5a17261de3d0544/index.ts#L34 https://github.com/jeemok/better-npm-audit/blob/fd99a0f41ff4342b8a0a6fdbe5a17261de3d0544/src/handlers/handleInput.ts#L30-L37 https://github.com/jeemok/better-npm-audit/issues/119 https://github.com/jeemok/better-npm-audit/pull/120 https://www.vulncheck.com/advisories/better-npm-audit-os-command-injection-via-registry-flag			
CVE-2026-61419	7,8	Dell ThinOS	Improper Access Control	versions prior to 2605_10.2518	https://www.dell.com/support/kbdoc/en-us/000496575/dsa-2026-350-security-update-for-dell-thinos-10-for-multiple-vulnerabilities	none	no	total
CVE-2026-68508	7,8	Hydra	Improper Control of Generation of Code ('Code Injection'); Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	Prior to 1.3.4	https://github.com/hydra-ecosystem/hydra/commit/7faad0dcedfb4c0a364aa1067c0080fd6fdf8dca https://github.com/hydra-ecosystem/hydra/issues/3259 https://github.com/hydra-ecosystem/hydra/pull/3261 https://github.com/hydra-ecosystem/hydra/releases/tag/v1.3.4 https://github.com/hydra-ecosystem/hydra/security/advisories/GHSA-2cp2-2r3c-7p7r	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-2026-68766	7,8	hashcat	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	7.1.2 and earlier	https://github.com/hashcat/hashcat https://github.com/hashcat/hashcat/blob/v7.1.2/src/restore.c#L365-L369 https://github.com/hashcat/hashcat/commit/fcae69f2438ff8eae0dc8e206b78067a1e465ed4 https://github.com/hashcat/hashcat/issues/4738 https://www.vulncheck.com/advisories/hashcat-through-arbitrary-file-write-via-restore-file-option-injection	poc	yes	partial
CVE-2026-74606	7,8	eventfs_remove_rec() eventfs_remove_rec() recursively removes the child at the current loop position		5dfb04100326f70e3b2d2872c2476ed20b804837 prior to b77581b25e213e83b79ce11eb30024e55ceeb3e9; 43aa6f97c2d03a52c1ddb86768575fc84344bdbb prior to f161d7861a0bfdf10af6b738b3b57636204661fb; 43aa6f97c2d03a52c1ddb86768575fc84344bdbb prior to 5635211b44969f4816e29ec4d5f8665fb39535d0; 43aa6f97c2d03a52c1ddb86768575fc84344bdbb prior to 74bb1eaf72d185a78c879eb2678ea500f82f46a8; 43aa6f97c2d03a52c1ddb86768575fc84344bdbb prior to fd73b691702170d37d66f4b0278530cea8ed419a; 5a43badefe0eccca0c26144c0a44b8d417ce8103; 6.6.18 prior to 6.6.152; 6.7.6 prior to 6.8; 6.8	https://git.kernel.org/stable/c/5635211b44969f4816e29ec4d5f8665fb39535d0 https://git.kernel.org/stable/c/74bb1eaf72d185a78c879eb2678ea500f82f46a8 https://git.kernel.org/stable/c/b77581b25e213e83b79ce11eb30024e55ceeb3e9 https://git.kernel.org/stable/c/f161d7861a0bfdf10af6b738b3b57636204661fb https://git.kernel.org/stable/c/fd73b691702170d37d66f4b0278530cea8ed419a			
CVE-2026-74640	7,8	fcp_meter_ctl_get() fcp_ioctl_set_meter_map()		> 255	https://git.kernel.org/stable/c/620f1e52a46f604635efd0fb78138afd6a513b5d https://git.kernel.org/stable/c/bb30e35c36ed00f24fa39aded811f64230a913b0 https://git.kernel.org/stable/c/bb61dc2ae59026f76db26e1909746908bc5b6f31			
CVE-2026-74674	7,8	direct page table reclaim When zap_pte_range reclaims a page table, it does: pte_free_tlb(tlb, pmd_pgtable(pmdval), addr)		4c640eb4181cf8de74c8b9e7c9cf16bf8d26b73e prior to 0b8ff21cbda8808c86b18f1b0ca2d0025af9a80a; 4c640eb4181cf8de74c8b9e7c9cf16bf8d26b73e prior to 478a1c3abebfc717db0d1281a9cdd7befafee542; 7.0	https://git.kernel.org/stable/c/0b8ff21cbda8808c86b18f1b0ca2d0025af9a80a https://git.kernel.org/stable/c/478a1c3abebfc717db0d1281a9cdd7befafee542			
CVE-2026-74675	7,8	kbd_keycode with tty_port_tty_get kbd_keycode() reads vc->port		1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to b84fd400f80adf4d1c88fbce50ae1cf2f8119e65; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to 38400673c9bfb39cfc87539e1a072087e98f4e4f; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to cab5a342f0589334046741006d8a280514f94235; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to 38a0aa593ebc275aea6f79534d07f44e43768ce6; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to 3f6b1d3fcfc26dc3fc85262f753439df93b055b4; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to b664592e9ba8c47c9e23408db7ba52eb9f946c8a; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to cc4a1a2ce0c58eafd477effb055863935260ddc1; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to e25d47a526939ad44b75f778b8a7500562b84fc1; 2.6.12	https://git.kernel.org/stable/c/38400673c9bfb39cfc87539e1a072087e98f4e4f https://git.kernel.org/stable/c/38a0aa593ebc275aea6f79534d07f44e43768ce6 https://git.kernel.org/stable/c/3f6b1d3fcfc26dc3fc85262f753439df93b055b4 https://git.kernel.org/stable/c/b664592e9ba8c47c9e23408db7ba52eb9f946c8a https://git.kernel.org/stable/c/b84fd400f80adf4d1c88fbce50ae1cf2f8119e65 https://git.kernel.org/stable/c/cab5a342f0589334046741006d8a280514f94235			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-74724	7,8	ip_vs_nat_icmp Sashiko warns that local attacker		1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to 3b8f79af0e98f27b932b0b416e9c52b692d31ff9; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to 3c779b258c9c3c3567af68d4f45c2f751f35bd0e; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to be65fa324640c7a95e30b146159a2be5cc73f22e; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to a69a4b3fff5814d079beff9a1e9d369994b2ed47; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to 243d0187ec4c3837b9b0004f18d1068e46115760; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to 646922a0379496154e8c8faca4f8e2fd9100cacc; 2.6.12	https://git.kernel.org/stable/c/243d0187ec4c3837b9b0004f18d1068e46115760 https://git.kernel.org/stable/c/3b8f79af0e98f27b932b0b416e9c52b692d31ff9 https://git.kernel.org/stable/c/3c779b258c9c3c3567af68d4f45c2f751f35bd0e https://git.kernel.org/stable/c/646922a0379496154e8c8faca4f8e2fd9100cacc https://git.kernel.org/stable/c/a69a4b3fff5814d079beff9a1e9d369994b2ed47 https://git.kernel.org/stable/c/be65fa324640c7a95e30b146159a2be5cc73f22e			
CVE-2026-76843	7,8	The official Flair wheels	Deserialization of Untrusted Data	0.15.0 through 0.15.1	https://github.com/flairNLP/flair https://github.com/flairNLP/flair/blob/v0.15.1/flair/models/clustering.py https://pypi.org/project/flair/0.15.1/ https://www.vulncheck.com/advisories/flair-and-deserialization-of-untrusted-data-via-clusteringmodel-load	none	no	total
CVE-2026-78136	7,8	chirpmyradio CHIRP	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	before 39178db	https://github.com/cduram/CHIRP-CodeExecution_via_Malicious_ImageFile https://github.com/kk7ds/chirp/commit/39178dbfc4fece083ab9ed20286d6ae3a91a718e	none	no	total
CVE-2026-78680	7,8	NLTK versions	Untrusted Search Path	versions before 3.10.3	https://github.com/nltk/nltk/security/advisories/GHSA-6hwm-xvph-95vm https://www.vulncheck.com/advisories/nltk-before-arbitrary-code-execution-via-graphviz-dot-binary			
CVE-2026-56707	7,7	Grav Flex Objects plugin	Missing Authorization	versions 1.4.0 through 1.4.7	https://github.com/getgrav/grav/security/advisories/GHSA-x929-528m-vx2m https://www.vulncheck.com/advisories/grav-flex-objects-through-authorization-bypass-via-shortcode			
CVE-2026-71366	7,7	multiple AWX notification backends	Server-Side Request Forgery (SSRF)		https://access.redhat.com/errata/RHSA-2026:59135 https://access.redhat.com/errata/RHSA-2026:59136 https://access.redhat.com/security/cve/CVE-2026-71366 https://bugzilla.redhat.com/show_bug.cgi?id=2511902			
CVE-2025-68825	7,5	HCL Hive	Incorrect Default Permissions	1.0	https://support.hcl-software.com/csm?id=kb_article&sysparm_article=KB0131731	none	yes	partial
CVE-2026-62243	7,5	netty	Improper Validation of Certificate with Host Mismatch	from 4.2.0.Final through 4.2.16.Final; through 4.1.136.Final	https://github.com/netty/netty/security/advisories/GHSA-p85m-gvr3-788c https://www.vulncheck.com/advisories/netty-through-tls-hostname-verification-bypass	none	yes	partial
CVE-2026-63421	7,5	Keystone	Improper Input Validation; Use of Incorrect Operator	Prior to 6.5.3	https://github.com/keystonejs/keystone/commit/9fb88b246950ce4de754a43fe6416f20403577b1 https://github.com/keystonejs/keystone/pull/9859 https://github.com/keystonejs/keystone/releases/tag/@keystone-6/core@6.5.3 https://github.com/keystonejs/keystone/security/advisories/GHSA-cqmq-8755-7xvh			
CVE-2026-66766	7,5	SAP S/4HANA (Private Cloud)	Inefficient Regular Expression Complexity	UIS4HOP1 800; 900	https://me.sap.com/notes/3771065 https://url.sap/sapsecuritypatchday			
CVE-2026-72700	7,5	The getgrav/grav-plugin-login Composer plugin	Observable Timing Discrepancy	before 3.9.1	https://github.com/getgrav/grav/security/advisories/GHSA-x239-6jqx-5hjh https://www.vulncheck.com/advisories/grav-before-timing-attack-via-non-constant-time-token-comparison			
CVE-2026-75899	7,5	fast-uri	Double Decoding of the Same Data; Server-Side Request Forgery (SSRF)	The affected versions are 2	https://cna.openjsf.org/security-advisories.html https://github.com/fastify/fast-uri/security/advisories/GHSA-fph4-wmhf-6fwf	none	yes	partial
CVE-2026-76098	7,5	Mistune	Uncontrolled Recursion	Versions 3.3.0 through 3.3.2	https://github.com/lepture/mistune/commit/0938fb7 https://github.com/lepture/mistune/security/advisories/GHSA-6m44-fpc8-c3rg	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-2026-76848	7,5	typeorm	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	0.2.21 through 1.1.0	https://github.com/typeorm/typeorm https://github.com/typeorm/typeorm/blob/1.1.0/src/query-builder/SelectQueryBuilder.ts https://www.vulncheck.com/advisories/typeorm-through-sql-injection-via-selectquerybuilder-distincton	none	yes	partial
CVE-2026-77384	7,5	libp2p	Uncontrolled Resource Consumption; Missing Release of Resource after Effective Lifetime	Prior to version 4.2.9	https://github.com/libp2p/js-libp2p/commit/4bb8fbe8d3f3590e4af51a1f5f7de56fffa5804d https://github.com/libp2p/js-libp2p/releases/tag/circuit-relay-v2-v4.2.9 https://github.com/libp2p/js-libp2p/security/advisories/GHSA-x787-qh7p-hmq7			
CVE-2026-78212	7,5	4MOSAn Management Center	Relative Path Traversal	prior to 20260621	https://www.twcert.org.tw/en/cp-139-11123-79a92-2.html https://www.twcert.org.tw/tw/cp-132-11119-25dfc-1.html	none	yes	partial
CVE-2026-78268	7,5	Lead Generation Contact Widget & AI Chatbot: Chat Button, Phone Call, Telegram, Email – SiteLeads	Exposure of Sensitive System Information to an Unauthorized Control Sphere	<= 1.2.0	https://patchstack.com/database/wordpress/plugin/siteleads/vulnerability/wordpress-lead-generation-contact-widget-ai-chatbot-chat-button-phone-call-telegram-email-siteleads-plugin-1-2-0-sensitive-data-exposure-vulnerability?_s_id=cve			
CVE-2026-76072	7,4	continue	Incomplete List of Disallowed Inputs	1.5.47 and earlier	https://github.com/continuedev/continue https://github.com/continuedev/continue/blob/main/packages/terminal-security/src/evaluateTerminalCommandSecurity.ts https://github.com/continuedev/continue/issues/13001 https://www.npmjs.com/package/@continuedev/cli https://www.vulncheck.com/advisories/continue-cli-through-incomplete-destructive-command-denylist-in-headless-and-auto-mode	poc	no	total
CVE-2026-76844	7,4	webpack-dev-middleware	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	5.3.4 through 5.3.4; 6.1.2 through 6.1.3; 7.1.0 through 7.4.5; 8.0.0 through 8.1.1	https://github.com/advisories/GHSA-wr3j-pwj9-hqq6 https://github.com/webpack/webpack-dev-middleware https://github.com/webpack/webpack-dev-middleware/blob/v8.1.1/src/middleware.js https://www.vulncheck.com/advisories/webpack-dev-middleware-path-traversal-via-offset-slice-on-a-non-slash-terminated-publicpath			
CVE-2026-19221	7,2	The Forminator Forms WordPress plugin	Improper Control of Generation of Code ('Code Injection')	before 1.57.0.5	https://wpscan.com/vulnerability/5aa85c72-2a60-4243-b370-ef0b46e98cfe/	none	no	total
CVE-2026-19685	7,1	NetworkManager	Incorrect Authorization		https://access.redhat.com/security/cve/CVE-2026-19685 https://bugzilla.redhat.com/show_bug.cgi?id=2515042 https://gitlab.freedesktop.org/NetworkManager/NetworkManager/-/commit/a8e87381a3e70060abd721d9a347f42b2ba68e6e https://gitlab.freedesktop.org/NetworkManager/NetworkManager/-/commit/e85cc46d0b36cdba50fe8411cc93d55a49ebfccf https://gitlab.freedesktop.org/NetworkManager/NetworkManager/-/merge_requests/2513	none	yes	total
CVE-2026-78367	7,0	RPM's rpmbuild tarball processing	Improper Control of Generation of Code ('Code Injection')		https://access.redhat.com/security/cve/CVE-2026-78367 https://bugzilla.redhat.com/show_bug.cgi?id=2521857 https://github.com/rpm-software-management/rpm/issues/4314	poc	no	total
CVE-2026-78465	7,0	the file-pcx plugin in GIMP	Integer Overflow or Wraparound		https://access.redhat.com/security/cve/CVE-2026-78465 https://bugzilla.redhat.com/show_bug.cgi?id=2522057 https://gitlab.gnome.org/GNOME/gimp/-/work_items/16578	poc	no	total

CISA/CERT-EU Alerts & Advisories

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

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds One Known Exploited Vulnerability to Catalog | CISA	▪ CVE-2026-21962 Oracle HTTP Server and Oracle Weblogic Server Proxy Plug-in Improper Access Control Vulnerability	https://cisa.gov/news-events/alerts/2026/08/24/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
TikTok reaches $400M settlement with US over COPPA violations	https://bleepingcomputer.com/news/legal/tiktok-reaches-400m-settlement-with-us-over-coppa-violations
ReliaQuest Confirms ShinyHunters Hack, but Says Impact Was Limited	https://securityweek.com/reliaquest-confirms-shinyhunters-hack-but-says-impact-was-limited
Microsoft Teams' New Policy Lets Admins Automatically Block Meeting Bots	https://cybersecuritynews.com/microsoft-teams-policy-to-block-bots
New Guidance Helps Businesses Verify Quantum-Safe Hardware Claims	https://infosecurity-magazine.com/news/guidance-verify-quantum-safe
NIST Warns of Unique Security Risks in Multi-Cloud Environments	https://infosecurity-magazine.com/news/nist-risks-multi-cloud
ReliaQuest confirms failed data-theft attack after ShinyHunters breach	https://bleepingcomputer.com/news/security/reliaquest-confirms-failed-data-theft-attack-after-shinyhunters-breach
Weekly Recap: AI-Powered PLC Attacks, GitLab Attacks, Stripe Key Leaks and More	https://thehackernews.com/2026/08/weekly-recap-ai-powered-plc-attacks.html
Microsoft Teams now lets admins block external bots from meetings	https://bleepingcomputer.com/news/security/microsoft-teams-now-lets-admins-block-external-bots-from-meetings
Hired for One Job, Judged on Another: The CISO's Real Problem	https://securityweek.com/hired-for-one-job-judged-on-another-the-cisos-real-problem
New Mysterious AI Model Dubbed Ox Alpha With Free 100 Trillion Tokens a Day for Coders	https://cybersecuritynews.com/new-mysterious-ai-model-dubbed-ox-alpha
Hackers Impersonate ReliaQuest Security Team Member to Steal SSO Credentials and MFA Access	https://cybersecuritynews.com/hackers-impersonate-reliaquest-security-staff
768 Leaked Corporate AWS Keys Remain Active With Full Administrator Access	https://cybersecuritynews.com/768-leaked-corporate-aws-keys-remain-active
Kimsuky Uses AI-Generated Chrome Extension to Automatically Steal Gmail Data	https://cybersecuritynews.com/kimsuky-ai-generated-chrome-extension

Doubloon Dredger Abuses Notion to Harvest Authentication Tokens	https://infosecurity-magazine.com/news/doubloon-dredger-notion
Uber Fined Nearly $1 Billion by Dutch Regulators Over Automated Suspensions of Driver Accounts	https://securityweek.com/uber-fined-nearly-1-billion-by-dutch-regulators-over-automated-suspensions-of-driver-accounts
Microsoft: August updates break printing, PDF export in WPF apps	https://bleepingcomputer.com/news/microsoft/microsoft-august-updates-break-printing-pdf-export-in-wpf-apps
The Outsized Shadow: Why 5% of AI Users Are Your Biggest Security Risk	https://thehackernews.com/2026/08/the-outsized-shadow-why-5-of-ai-users.html
Venezuelan Gets Record Federal Prison Term for ATM Jackpotting	https://securityweek.com/venezuelan-gets-record-federal-prison-term-for-atm-jackpotting
Rethinking Application Security for the AI Era	https://securityweek.com/rethinking-application-security-for-the-ai-era
Microsoft shares temporary fix for Windows 11 gaming issues	https://bleepingcomputer.com/news/microsoft/microsoft-shares-temporary-fix-for-windows-11-gaming-issues

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
Personal Information Exposed in Apollo Global Data Breach	https://securityweek.com/personal-information-exposed-in-apollo-global-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
Multiple TP-Link Archer Vulnerabilities Enable Command Injection Attacks	https://cybersecuritynews.com/tp-link-archer-command-injection-flaw
Actively Exploited Oracle WebLogic Flaw Lets Unauthenticated Attackers Access Critical Data	https://thehackernews.com/2026/08/actively-exploited-oracle-weblogic-flaw.html
Researcher Discloses Five High-Risk Vulnerabilities in Palo Alto GlobalProtect VPN	https://cybersecuritynews.com/5-vulnerabilities-palo-alto-globalprotect
Exploited Zimbra Flaw Highlights Shrinking Window to Patch	https://darkreading.com/vulnerabilities-threats/zimbra-flaw-exploitation-shrinking-window-patch
Hackers target WordPress sites in miniOrange auth bypass attacks	https://bleepingcomputer.com/news/security/hackers-target-wordpress-sites-in-miniorange-auth-bypass-attacks
Zimbra Collaboration Suite Vulnerability Actively Exploited in the Wild	https://cybersecuritynews.com/zimbra-collaboration-suite-vulnerability-exploited
The Vulnerability Gap: Why Discovery Is Outrunning Repair	https://darkreading.com/cybersecurity-operations/vulnerability-gap-why-discovery-is-outrunning-repair
WordPress Plugin Vulnerability Exposes 100,000 Sites to Complete Site Takeover Attacks	https://cybersecuritynews.com/wordpress-everest-forms-plugin-flaw

Critical Keycloak Password Reset Flaw Could Let Unauthenticated Attackers Take Over Any Account	https://thehackernews.com/2026/08/critical-keycloak-password-reset-flaw.html
CISA orders urgent patching of actively exploited Zimbra flaw	https://bleepingcomputer.com/news/security/cisa-orders-urgent-patching-of-actively-exploited-zimbra-flaw
Critical isolated-vm Flaw Lets Untrusted JavaScript Escape Sandbox and Hijack Host Execution	https://cybersecuritynews.com/critical-isolated-vm-flaw
What 45 Million wp2shell Exploit Attempts Reveal About the New Vulnerability Response Window	https://cybersecuritynews.com/what-45-million-wp2shell-exploit-attempts-reveal-about-the-new-vulnerability-response-window

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
Unpatched Calix flaw lets hackers bypass NAT to expose internal devices	https://bleepingcomputer.com/news/security/unpatched-calix-flaw-lets-hackers-bypass-nat-to-expose-internal-devices
91 Vulnerabilities Patched in Spring Application Framework	https://securityweek.com/91-vulnerabilities-patched-in-spring-application-framework

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
Tricky 'SynkLoader' Multitool May Herald Ransomware	https://darkreading.com/threat-intelligence/tricky-synkloader-multitool-ransomware
Fake Codex Download Uses Google Sites to Deliver macOS Malware	https://infosecurity-magazine.com/news/fake-codex-download-google-sites
Hackers Poison Google and Bing Results to Deliver Cloaked Banking Phishing Pages	https://cybersecuritynews.com/hackers-poison-google-bing-results
Microsoft Teams Phishing Deploys New SynkLoader Malware to Steal Windows Passwords	https://cybersecuritynews.com/microsoft-teams-phishing
UAT-10147 Uses AI to Scale Server Attacks, Deploys SPECTRE With EDR Bypass and Linux Rootkit	https://thehackernews.com/2026/08/uat-10147-uses-ai-to-scale-server.html
Hackers Infect Android Car Screens Through Their Built-In Software Update System	https://cybersecuritynews.com/hackers-infect-android-car-screens
New Malware-as-a-service Leveraging Adobe-themed Domain to Attack Windows Users Using .bat File	https://cybersecuritynews.com/malware-as-a-service-adobe-themed-domain
Weekly Cyber Security Newsletter Bulletin – Entra ID RCE, Claude Code Ransomware, T-Mobile Cable, Azure Credential Theft +20 Stories	https://cybersecuritynews.com/cyber-security-newsletter-bulletin-august
ToxicPanda Android malware uses VPN permissions to block Google Play	https://bleepingcomputer.com/news/security/toxicpanda-android-malware-uses-vpn-permissions-to-block-google-play

Hackers infect Android car head units with proxy botnet malware	https://bleepingcomputer.com/news/security/hackers-infect-android-car-head-units-with-proxy-botnet-malware

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 22/08/2026–25/08/2026, 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/