

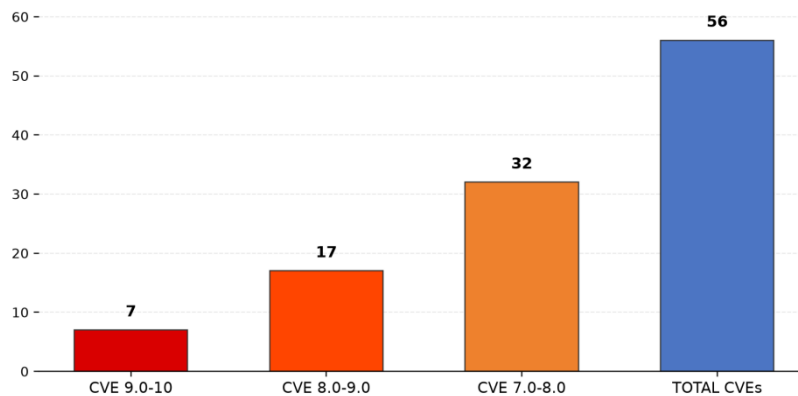


Newsletter on system vulnerabilities and
cybersecurity news.

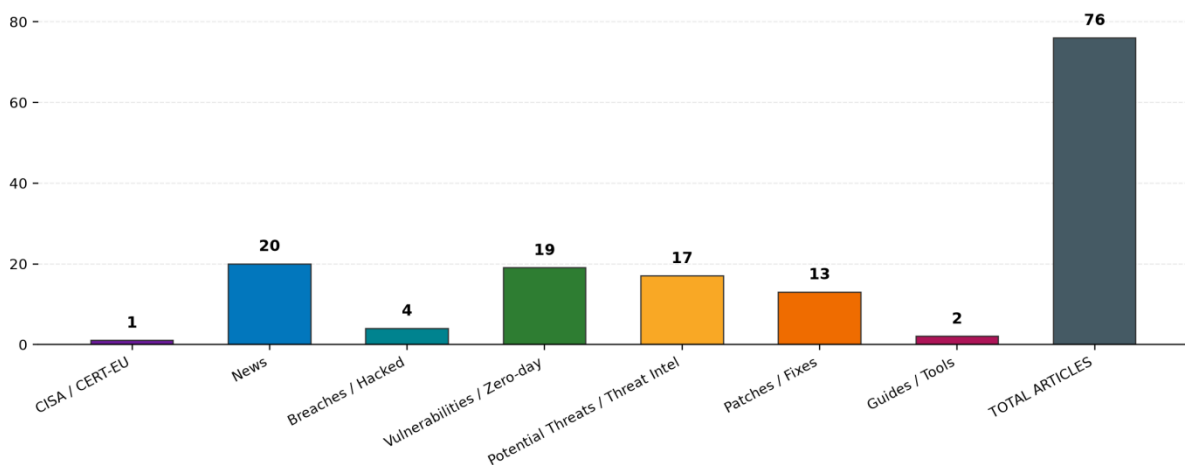
National Cyber Security Authority (NCSA)

Date: 23/09/2026 - 25/09/2026

of CVEs per CVSS score



of articles per section



Contents

Common Vulnerabilities and Exposures (CVEs)	3
CISA/CERT-EU Alerts & Advisories	16
News.....	16
Breaches / Compromised / Hacked.....	17
Vulnerabilities / Flaws / Zero-day.....	17
Patches / Updates / Fixes	18
Potential threats / Threat intelligence	19
Guides / Tools.....	20
References.....	21
Annex – Websites with vendor specific vulnerabilities	22

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-2026-61732	10,0	Decepticon	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	Versions prior to 1.1.17	https://github.com/BitterSecurity/Decepticon/commit/79ee2aaf22f4c36a5b1968f6ca3f8086b6e35b67 https://github.com/BitterSecurity/Decepticon/security/advisories/GHSA-q5f9-3xfq-p9mf	poc	yes	total
CVE-2026-14281	9,8	The Automation Web Platform – Notifications and OTP for WooCommerce, Advanced Country Code plugin for WordPress	Improper Privilege Management	up to, and including, 4.8.6.	https://plugins.trac.wordpress.org/browser/automation-web-platform/tags/4.8.6/includes/api/class-wawp-rest-settings-api.php#L342 https://plugins.trac.wordpress.org/browser/automation-web-platform/tags/4.8.6/includes/api/class-wawp-rest-settings-api.php#L574 https://plugins.trac.wordpress.org/browser/automation-web-platform/tags/4.8.6/includes/auth-services/class-wawp-otp-service.php#L477 https://plugins.trac.wordpress.org/browser/automation-web-platform/tags/4.8.6/includes/auth-services/class-wawp-otp-service.php#L787 https://plugins.trac.wordpress.org/browser/automation-web-platform/tags/4.8.6/includes/auth-services/class-wawp-signup.php#L1002 https://plugins.trac.wordpress.org/browser/automation-web-platform/tags/4.8.6/includes/auth-services/class-wawp-signup.php#L845			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-93207	9,8	Linux		b0bc53470d1af01f62a0 fe2d405cf56477804863 prior to 56b29d62017c7dd1718 d060dd5b3a2ce61095d 0c; b0bc53470d1af01f62a0 fe2d405cf56477804863 prior to 0e18641708eaa8bc3c1f f338cd844aeaddb52bac ; b0bc53470d1af01f62a0 fe2d405cf56477804863 prior to e0778464049b0238f29 15a40007a4154f86cf35 1; b0bc53470d1af01f62a0 fe2d405cf56477804863 prior to 0fa8a8acae57e637396 2741d5b06d13f44aba6 a9; b0bc53470d1af01f62a0 fe2d405cf56477804863 prior to 11539e8fcce0b0af062a e5fecf7b3676c2f7aeed; 6.3	https://git.kernel.org/stable/c/0e18641708eaa8bc3c1ff338cd844aeaddb52bac https://git.kernel.org/stable/c/0fa8a8acae57e6373962741d5b06d13f44aba6a9 https://git.kernel.org/stable/c/11539e8fcce0b0af062ae5fecf7b3676c2f7aeed https://git.kernel.org/stable/c/56b29d62017c7dd1718d060dd5b3a2ce61095d0c https://git.kernel.org/stable/c/e0778464049b0238f2915a40007a4154f86cf351			
CVE-2026-61741	9,3	http4s-scala.xml	Improper Restriction of XML External Entity Reference	< 0.24.1; >= 1.0.0-M1, < 1.0.0-M39	https://github.com/http4s/http4s-scala-xml/security/advisories/GHSA-cjx3-73hr-rpw7			
CVE-2026-79766	9,1	Termix	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	>= 2.4.1, < 2.5.1	https://github.com/Termix-SSH/Termix/commit/c7a9063a72071153723e668787548766c971f029 https://github.com/Termix-SSH/Termix/commit/ddbdd5c437c2296607d4aa4265d6f63fbc1ca92e https://github.com/Termix-SSH/Termix/pull/1067 https://github.com/Termix-SSH/Termix/releases/tag/release-2.5.1-tag https://github.com/Termix-SSH/Termix/security/advisories/GHSA-pr55-25qf-5f9v			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-89055	9,1	The Customer Reviews for WooCommerce plugin for WordPress; all	Missing Authorization	up to, and including, 5.120.0.	https://plugins.trac.wordpress.org/browser/customer-reviews-woocommerce/tags/5.120.0/includes/reminders/class-cr-local-forms-ajax.php#L57 https://plugins.trac.wordpress.org/browser/customer-reviews-woocommerce/tags/5.120.0/includes/reviews/class-cr-endpoint.php#L318 https://plugins.trac.wordpress.org/browser/customer-reviews-woocommerce/tags/5.120.0/includes/reviews/class-cr-endpoint.php#L467 https://plugins.trac.wordpress.org/browser/customer-reviews-woocommerce/tags/5.120.0/includes/reviews/class-cr-reviews.php#L129 https://plugins.trac.wordpress.org/browser/customer-reviews-woocommerce/tags/5.120.0/includes/reviews/class-cr-reviews.php#L1871 https://plugins.trac.wordpress.org/changeset?reponame=&old=3694303%40customer-reviews-woocommerce&new=3694303%40customer-reviews-woocommerce			
CVE-2026-93399	9,1	The Bookly plugin for WordPress	Authorization Bypass Through User-Controlled Key	up to, and including, 28.2	https://plugins.trac.wordpress.org/browser/bookly-responsive-appointment-booking-tool/tags/28.2/frontend/modules/booking/Ajax.php#L1111 https://plugins.trac.wordpress.org/browser/bookly-responsive-appointment-booking-tool/tags/28.2/frontend/modules/booking/Ajax.php#L46 https://plugins.trac.wordpress.org/browser/bookly-responsive-appointment-booking-tool/tags/28.2/frontend/modules/booking/Ajax.php#L733 https://plugins.trac.wordpress.org/browser/bookly-responsive-appointment-booking-tool/tags/28.2/frontend/modules/payment/Ajax.php#L74 https://plugins.trac.wordpress.org/browser/bookly-responsive-appointment-booking-tool/tags/28.2/lib/UserBookingData.php#L360 https://plugins.trac.wordpress.org/browser/bookly-responsive-appointment-booking-tool/tags/28.2/lib/base/Gateway.php#L301			
CVE-2026-94606	8,9	authentik	Improper Authentication; Reliance on Untrusted Inputs in a Security Decision	Prior to 2026.2.7, 2026.5.7	https://docs.goauthentik.io/releases/2026.2#fixed-in-202627 https://docs.goauthentik.io/releases/2026.5#fixed-in-202657 https://docs.goauthentik.io/releases/2026.8#fixed-in-202682 https://github.com/goauthentik/authentik/commit/01d4349f2aaa9beda532f92e2a251a17fefee9b3 https://github.com/goauthentik/authentik/commit/1fcf9868133e5d05e266edbc1f6f3ee972baa3f9 https://github.com/goauthentik/authentik/commit/c10ae83ebf8c61de2f1922edf1fab504d9f3b06f			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-19804	8,8	s2Member – Excellent for All Kinds of Memberships, Content Restriction Paywalls & Member Access Subscriptions	Improper Control of Generation of Code ('Code Injection')	up to, and including, 260814	https://plugins.trac.wordpress.org/browser/s2member/trunk/src/includes/classes/paypal-checkout-in.inc.php#L736 https://plugins.trac.wordpress.org/browser/s2member/trunk/src/includes/classes/paypal-return-in-subscr-or-wa-w-level.inc.php#L311 https://plugins.trac.wordpress.org/browser/s2member/trunk/src/includes/classes/paypal-return-in-subscr-or-wa-w-level.inc.php#L319 https://plugins.trac.wordpress.org/browser/s2member/trunk/src/includes/classes/paypal-return-in.inc.php#L47 https://plugins.trac.wordpress.org/browser/s2member/trunk/src/includes/classes/paypal-utilities.inc.php#L185 https://plugins.trac.wordpress.org/browser/s2member/trunk/src/includes/classes/paypal-utilities.inc.php#L92			
CVE-2026-62062	8,8	Elementor Website Builder	Cross-Site Request Forgery (CSRF)	through 4.3.1.	https://patchstack.com/database/wordpress/plugin/elementor/vulnerability/wordpress-elementor-website-builder-plugin-4-3-1-cross-site-request-forgery-csrf-vulnerability?s_id=cve			
CVE-2026-89426	8,8	The Knit Pay – Cashfree, Instamojo, Razorpay, PayPal and more plugin for Word-Press	Improper Privilege Management	up to, and including, 9.6.1.0.	https://plugins.trac.wordpress.org/browser/knit-pay/tags/9.4.0.1/packages/wp-pay-extensions/gravityforms/src/Extension.php#L381 https://plugins.trac.wordpress.org/browser/knit-pay/tags/9.4.0.1/packages/wp-pay-extensions/gravityforms/src/Extension.php#L384 https://plugins.trac.wordpress.org/browser/knit-pay/tags/9.4.0.1/packages/wp-pay-extensions/gravityforms/src/Extension.php#L989 https://plugins.trac.wordpress.org/browser/knit-pay/tags/9.4.0.1/packages/wp-pay-extensions/gravityforms/src/Processor.php#L493 https://plugins.trac.wordpress.org/browser/knit-pay/tags/9.6.1.0/packages/wp-pay-extensions/gravityforms/src/Extension.php#L381 https://plugins.trac.wordpress.org/browser/knit-pay/tags/9.6.1.0/packages/wp-pay-extensions/gravityforms/src/Extension.php#L384			
CVE-2026-96883	8,8	pgcollection	Access of Resource Using Incompatible Type ('Type Confusion')	2.0.0 through 2.1.1; 2.1.2 or later	https://aws.amazon.com/security/security-bulletins/2026-118-aws/ https://github.com/aws/pgcollection/releases/tag/v2.1.2 https://github.com/aws/pgcollection/security/advisories/GHSA-q539-cj32-hv6r	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-2026-97409	8,8	io target		1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to da930308b4bc24c335574e85ca84ff70a988cf05 ; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to dd39064d2948b14dbe4f364fe4b3c9cfc632cc21 ; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to ee38469f88492df99e1d97f03aa40ecfd218934f; prior to 6.12.111; prior to 6.18.53	https://git.kernel.org/stable/c/da930308b4bc24c335574e85ca84ff70a988cf05 https://git.kernel.org/stable/c/dd39064d2948b14dbe4f364fe4b3c9cfc632cc21 https://git.kernel.org/stable/c/ee38469f88492df99e1d97f03aa40ecfd218934f			
CVE-2026-61825	8,7	code16 Sharp	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Versions before 9.22.5	https://github.com/code16/sharp/commit/ec509a22c808a5bd9dfad6a0a85c92ce6f411e21 https://github.com/code16/sharp/security/advisories/GHSA-vi3q-vp3g-l9c8	none	no	total
CVE-2026-63498	8,7	Snipe-IT	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Prior to 8.7.0	https://github.com/grokability/snipe-it/commit/e929b31f0b183c5810bd2b833c1f6f643cbe5284 https://github.com/grokability/snipe-it/releases/tag/v8.7.0 https://github.com/grokability/snipe-it/security/advisories/GHSA-396x-xmvy-p563			
CVE-2026-77581	8,6	BentoPDF	Server-Side Request Forgery (SSRF)	2.8.6 and earlier	https://github.com/alam0000/bentopdf/commit/45496fcd2ed6e02dcdde0d3839cc5024c091760c https://github.com/alam0000/bentopdf/commit/58cd1a8893bfe06e4a59a72adc2e7db00a8b9266 https://github.com/alam0000/bentopdf/releases/tag/v2.8.7 https://github.com/alam0000/bentopdf/security/advisories/GHSA-5xif-rr5x-pcfj	poc	yes	partial
CVE-2026-97818	8,6	phpIPAM	Incorrect Authorization	through 1.8.3	https://github.com/phpipam/phpipam/blob/e8010751d491e485acefa5787fb0e518eb948771/api/controllers/Us er.php#L143-L146 https://github.com/phpipam/phpipam/releases/tag/v1.8.3			
CVE-2026-76086	8,5	Formie	Missing Authorization; Improperly Controlled Modification of Dynamically-Determined Object Attributes; Server-Side Request Forgery (SSRF)	Prior to 2.2.23 and 3.1.31	https://github.com/advisories/GHSA-cvpc-hccg-wmw4 https://github.com/verbb/formie/commit/6735fe4ae8f6a2a76930716ad7876b236f7c530d https://github.com/verbb/formie/commit/dde7799dfa7e4d0a11e28754ad8544dba62d5def https://github.com/verbb/formie/releases/tag/2.2.23 https://github.com/verbb/formie/releases/tag/3.1.31 https://github.com/verbb/formie/security/advisories/GHSA-v3f3-cmi4-cvi9			
CVE-2026-97730	8,5	In Netgate pfSense Plus	Path Traversal: '../filedir'	before 26.07; before 2.9.0	https://docs.netgate.com/downloads/pfSense-SA-26-18.webqui.asc https://docs.netgate.com/pfsense/en/latest/install/upgrade-guide.html https://redmine.pfsense.org/attachments/7146 https://redmine.pfsense.org/issues/16947			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-97451	8,4	acpi_ex_op-code_3A_1T_1R() (mid_op) Add overflow check for Index + Length to prevent integer overflow when calculating the truncation length		1da177e4c3f41524e886b7f1b8a0c1fc7321cac 2 prior to d0d89f2e16a874e0f8fb17045da293e8bedf8b21; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac 2 prior to b96401812cbfb4803faabeefa1f20b8562268b3; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac 2 prior to 0e2021f49e64b3c8a9aa880d0c62a218bfe147ce; prior to 6.12.111; prior to 6.18.53	https://git.kernel.org/stable/c/0e2021f49e64b3c8a9aa880d0c62a218bfe147ce https://git.kernel.org/stable/c/b96401812cbfb4803faabeefa1f20b8562268b3 https://git.kernel.org/stable/c/d0d89f2e16a874e0f8fb17045da293e8bedf8b21			
CVE-2026-91160	8,2	OpenWA	Missing Authorization	Prior to 0.23.5	https://github.com/rmyndharis/OpenWA/commit/acc23c3803c07f43791a92e8e48456572fd69bdc https://github.com/rmyndharis/OpenWA/commit/b9d9ea1c57bde98b7833a5d6e482998703667ef0 https://github.com/rmyndharis/OpenWA/pull/1602 https://github.com/rmyndharis/OpenWA/releases/tag/v0.23.5 https://github.com/rmyndharis/OpenWA/security/advisories/GHSA-m427-j4h4-9gwl			
CVE-2026-77294	8,1	TREK	Server-Side Request Forgery (SSRF)	Prior to 3.3.0	https://github.com/liketrek/TREK/commit/19064b39176660f3be3a2df198c87949504046e2 https://github.com/liketrek/TREK/pull/1520 https://github.com/liketrek/TREK/releases/tag/v3.3.0 https://github.com/liketrek/TREK/security/advisories/GHSA-fmq9-qgh3-647p	poc	no	total
CVE-2026-92713	8,1	The Modula Image Gallery – Photo Grid & Video Gallery plugin for WordPress	Missing Authorization	up to, and including, 3.0.2.	https://plugins.trac.wordpress.org/browser/modula-best-grid-gallery/tags/3.0.2/includes/admin/helpers/class-modula-gallery-upload.php#L1310 https://plugins.trac.wordpress.org/browser/modula-best-grid-gallery/tags/3.0.2/includes/admin/helpers/class-modula-gallery-upload.php#L260 https://plugins.trac.wordpress.org/browser/modula-best-grid-gallery/tags/3.0.2/includes/v2/rest/class-gallery-upload-controller.php#L337 https://plugins.trac.wordpress.org/changeset?reponame=&old=3701804%40modula-best-grid-gallery&new=3701804%40modula-best-grid-gallery https://www.wordfence.com/threat-intel/vulnerabilities/id/1686f4ad-b114-4e4f-b8f7-8ea7c31b2672?source=cve			
CVE-2026-97735	8,0	ITFlow	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	before 26.08	https://github.com/itflow-org/itflow/commit/16000efcf7f7c833aae9f8da22d2a82df21a49c0 https://github.com/itflow-org/itflow/security/advisories/GHSA-89fw-w69c-vqhl			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-93798	7,8	merge_reloc_roots() If the root we got		1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to ab48583aa9948205ff9a6470e23dbff74c565e24 ; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to 63d6b1f04cd91c825329712aa526215ffa5d11ca ; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to b78fe9563e2d5ae47805f1e5dc722c91fd30e1f8 ; prior to 6.12.111; prior to 6.18.53	https://git.kernel.org/stable/c/63d6b1f04cd91c825329712aa526215ffa5d11ca https://git.kernel.org/stable/c/ab48583aa9948205ff9a6470e23dbff74c565e24 https://git.kernel.org/stable/c/b78fe9563e2d5ae47805f1e5dc722c91fd30e1f8			
CVE-2026-97429	7,8	de-destroy_queue_cpsh wait_on_de-destroy_queue() drops locks to wait for queue resume, allowing a concurrent destroy to free the queue		1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to 41144829f4645c2bd4cb501d34d253858f750c0a ; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to d98c8032c29944e1e572e1f49a0613d364fece0f ; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to ac081deaf16a639ea7df2f285fe421a33c1ade0; prior to 6.12.111; prior to 6.18.53	https://git.kernel.org/stable/c/41144829f4645c2bd4cb501d34d253858f750c0a https://git.kernel.org/stable/c/ac081deaf16a639ea7df2f285fe421a33c1ade0 https://git.kernel.org/stable/c/d98c8032c29944e1e572e1f49a0613d364fece0f			
CVE-2026-97444	7,7	two places Add boundary checks in acpi_ps_get_next_namestring() and acpi_ps_peek_opcode() to prevent out-of-bounds access		1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to 253d7272d01db9529c79b95205c0f859ef9f4f23 ; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to 4de2cffe5e6b5b79eec8c934df582459b818228; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 prior to bdc35754012906dbf094be104b103ca3ad-fef6f7; prior to 6.12.111; prior to 6.18.53	https://git.kernel.org/stable/c/253d7272d01db9529c79b95205c0f859ef9f4f23 https://git.kernel.org/stable/c/4de2cffe5e6b5b79eec8c934df582459b818228 https://git.kernel.org/stable/c/bdc35754012906dbf094be104b103ca3ad-fef6f7			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-97448	7,7	acpi_ns_build_normalized_path() Add validation for node in acpi_ns_build_normalized_path() to prevent use-after-free vulnerabilities		1da177e4c3f41524e886b7f1b8a0c1fc7321cac 2 prior to babb146ceb79e71f328788f1e2c8c7c224026e61; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac 2 prior to 21a73528579fcbd673b668bd27a05b658123bc1b; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac 2 prior to 96b2b616870e46e2bc04efec03879683a0036e66; prior to 6.12.111; prior to 6.18.53	https://git.kernel.org/stable/c/21a73528579fcbd673b668bd27a05b658123bc1b https://git.kernel.org/stable/c/96b2b616870e46e2bc04efec03879683a0036e66 https://git.kernel.org/stable/c/babb146ceb79e71f328788f1e2c8c7c224026e61			
CVE-2026-97454	7,7	acpi_ps_get_next_field() Add boundary checks in acpi_ps_get_next_field() to prevent out-of-bounds access		1da177e4c3f41524e886b7f1b8a0c1fc7321cac 2 prior to add715fc1ef5b0a71afe22b3f02aa28775d9ba62; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac 2 prior to bc5b2158c7626e3e8a78c5bb93ce0a734a26b84a; 1da177e4c3f41524e886b7f1b8a0c1fc7321cac 2 prior to e15aa60de0256d63df2331bf5a4bc4dd287504cd; prior to 6.12.111; prior to 6.18.53	https://git.kernel.org/stable/c/add715fc1ef5b0a71afe22b3f02aa28775d9ba62 https://git.kernel.org/stable/c/bc5b2158c7626e3e8a78c5bb93ce0a734a26b84a https://git.kernel.org/stable/c/e15aa60de0256d63df2331bf5a4bc4dd287504cd			
CVE-2026-13456	7,5	The WP Maps – Google Maps, OpenStreetMap, Mapbox, Store Locator, Listing, Directory & Filters plugin for WordPress	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')	up to, and including, 4.9.8	https://plugins.trac.wordpress.org/browser/wp-google-map-plugin/tags/4.9.3/core/class.controller.php#L115 https://plugins.trac.wordpress.org/browser/wp-google-map-plugin/tags/4.9.3/wp-google-map-plugin.php#L605 https://plugins.trac.wordpress.org/browser/wp-google-map-plugin/tags/4.9.3/wp-google-map-plugin.php#L622 https://plugins.trac.wordpress.org/browser/wp-google-map-plugin/tags/4.9.5/core/class.controller.php#L115 https://plugins.trac.wordpress.org/browser/wp-google-map-plugin/tags/4.9.5/wp-google-map-plugin.php#L605 https://plugins.trac.wordpress.org/browser/wp-google-map-plugin/tags/4.9.5/wp-google-map-plugin.php#L622			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-57440	7,5	The EmbedVideo Extension	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'); Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	Prior to 4.1.0; Version 4.1.0	https://github.com/StarCitizenWiki/mediawiki-extensions-EmbedVideo/commit/370156335b325bb81d14d89edf0a1f2643d50a84 https://github.com/StarCitizenWiki/mediawiki-extensions-EmbedVideo/security/advisories/GHSA-v65j-hff3-753c			
CVE-2026-59990	7,5	Jawn	Allocation of Resources Without Limits or Throttling	Prior to 1.7.0	https://github.com/typelevel/jawn/commit/191cb3a44e77f1afab439ee636bf66bdf3c54a04 https://github.com/typelevel/jawn/commit/6219666641f9408498f85868f835e17bd8a72fed https://github.com/typelevel/jawn/commit/93ac93e9c992c11b4c03d5455d8551f9fb24da1b https://github.com/typelevel/jawn/commit/f6ace7e0db715de1a8c4618bed9378333a5c2214 https://github.com/typelevel/jawn/releases/tag/v1.7.0 https://github.com/typelevel/jawn/security/advisories/GHSA-cc4v-rvqp-2pf3	none	yes	partial
CVE-2026-61695	7,5	Wire	Improper Validation of Array Index	Prior to 6.4.1 and 7.0.0-alpha04	https://github.com/square/wire/commit/24043b6b3a5e5974a978f2745b76d50b31407c1c https://github.com/square/wire/commit/81ff7f24a6795d9a8be2e03f272b2d979a5d2c7e https://github.com/square/wire/pull/3616 https://github.com/square/wire/releases/tag/6.4.1 https://github.com/square/wire/releases/tag/7.0.0-alpha04 https://github.com/square/wire/security/advisories/GHSA-A-86wm-r4c5-2rc9			
CVE-2026-61782	7,5	Rsdctor	Exposure of Sensitive Information to an Unauthorized Actor	Prior to version 1.5.16	https://github.com/web-infra-dev/rsdoctor/security/advisories/GHSA-jmq2-rcxh-w8g3			
CVE-2026-61816	7,5	zbateson/mail-mime-parser	Uncontrolled Resource Consumption	in version 2.0.0 and prior; Versions prior to 2.0	https://github.com/zbateson/mail-mime-parser/security/advisories/GHSA-f6v3-2qmr-vfjx	poc	yes	partial
CVE-2026-63645	7,5	OpenObserve	Exposure of Sensitive Information to an Unauthorized Actor	Prior to 0.90.3	https://github.com/openobserve/openobserve/commit/4f3db1cf790ffe8ea065d98f87344e839ec6e477 https://github.com/openobserve/openobserve/pull/12220 https://github.com/openobserve/openobserve/releases/tag/v0.90.3 https://github.com/openobserve/openobserve/security/advisories/GHSA-v496-q5c9-vqxw			
CVE-2026-71540	7,5	Wazuh	Allocation of Resources Without Limits or Throttling	up to 256	https://github.com/wazuh/wazuh/commit/9a996bc23d28725f6c1f8f7808355d90e20d3382 https://github.com/wazuh/wazuh/pull/37280 https://github.com/wazuh/wazuh/releases/tag/v4.14.7 https://github.com/wazuh/wazuh/security/advisories/GHSA-78wx-4r6w-w73f			
CVE-2026-75907	7,5	The door access control on a Norwegian Cruise Line asset grants entry based only on the credential's static	Improper Authentication; Authentication Bypass by Capture-replay; Insufficient Session Expiration		https://kb.cert.org/vuls/id/676317 https://www.kb.cert.org/vuls/id/676317	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-2026-77422	7,5	JLine	Inefficient Regular Expression Complexity	>= 3.0.0, < 3.30.15; >= 4.0.0, < 4.3.1	https://github.com/ljline/jline3/commit/1d5fc3099e77938b971e197211cad2d4fbb17541 https://github.com/ljline/jline3/commit/341ee69ccc57b7733c1b40d6993219b64b3206ae https://github.com/ljline/jline3/pull/2012 https://github.com/ljline/jline3/pull/2018 https://github.com/ljline/jline3/releases/tag/4.3.1 https://github.com/ljline/jline3/releases/tag/jline-3.30.15	poc	yes	partial
CVE-2026-82356	7,5	Imprivata Enterprise Access Management	Inadequate Encryption Strength; Use of a Broken or Risky Cryptographic Algorithm	<=26.2	https://kb.cert.org/vuls/id/273940 https://www.kb.cert.org/vuls/id/273940	none	yes	partial
CVE-2026-57178	7,4	Python Social Auth	Improper Authentication; Improper Verification of Cryptographic Signature	Prior to version 5.0.0	https://github.com/pythonsocial-auth/social-core/security/advisories/GHSA-3c93-f73f-qc9h			
CVE-2026-61788	7,4	DBHub	Incomplete List of Disallowed Inputs; Not Failing Securely ('Failing Open'); Incorrect Authorization	Prior to version 0.22.6	https://github.com/bytebase/dbhub/security/advisories/GHSA-mwwr-p57h-56pf			
CVE-2026-97737	7,4	In Wakapi	Access of Resource Using Incompatible Type ('Type Confusion')	before 2.17.6	https://github.com/muety/wakapi/commit/ce91eac2c2d9b29a00873554d2ecef76f10b9087 https://github.com/muety/wakapi/releases/tag/2.17.6 https://github.com/muety/wakapi/security/advisories/GHSA-x48w-3rq3-w2pg			
CVE-2026-97646	7,3	ningzichun student-management-system	Improper Authorization; Authorization Bypass Through User-Controlled Key	up to 98760f5711cf6dc8b4adca53a9e207ca49b02ebf	https://github.com/ningzichun/student-management-system/ https://github.com/ningzichun/student-management-system/issues/9 https://vuldb.com/cve/CVE-2026-97646 https://vuldb.com/submit/910054 https://vuldb.com/vuln/409748 https://vuldb.com/vuln/409748/cti			
CVE-2026-83591	7,2	The AMP for WP – Accelerated Mobile Pages plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 1.1.16	https://plugins.trac.wordpress.org/browser/accelerated-mobile-pages/tags/1.1.14/components/comments/comments.php#L89 https://plugins.trac.wordpress.org/browser/accelerated-mobile-pages/tags/1.1.14/includes/features/functions.php#L314 https://plugins.trac.wordpress.org/browser/accelerated-mobile-pages/tags/1.1.14/templates/features.php#L8823 https://plugins.trac.wordpress.org/browser/accelerated-mobile-pages/tags/1.1.15/components/comments/comments.php#L89 https://plugins.trac.wordpress.org/browser/accelerated-mobile-pages/tags/1.1.15/includes/features/functions.php#L314 https://plugins.trac.wordpress.org/browser/accelerated-mobile-pages/tags/1.1.15/templates/features.php#L8823			
CVE-2026-84279	7,2	The Fancy Product Designer plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 6.5.2	https://fancyproductdesigner.com/ https://www.wordfence.com/threat-intel/vulnerabilities/id/aa9e0489-effd-4235-a6a9-2bece0fe2abf?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-2026-93303	7,2	The HT Contact Form – Drag & Drop Form Builder for WordPress plugin for Word-Press	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 2.10.1	https://plugins.trac.wordpress.org/browser/ht-contactform/tags/2.10.1/admin/Includes/Api/Endpoints/Draft.php#L199 https://plugins.trac.wordpress.org/browser/ht-contactform/tags/2.10.1/admin/Includes/Api/Endpoints/Draft.php#L336 https://plugins.trac.wordpress.org/browser/ht-contactform/tags/2.10.1/admin/Includes/Api/Endpoints/Draft.php#L74 https://plugins.trac.wordpress.org/browser/ht-contactform/tags/2.10.1/admin/Includes/Models/Drafts.php#L239 https://plugins.trac.wordpress.org/browser/ht-contactform/tags/2.10.1/assets/js/form.js#L2053 https://plugins.trac.wordpress.org/browser/ht-contactform/tags/2.10.1/include/UI/ShortCode.php#L726			
CVE-2026-93654	7,2	The Premium Packages – Sell Digital Products Securely plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 7.2.1	https://plugins.trac.wordpress.org/browser/wpdm-premium-packages/tags/7.2.1/includes/libs/cart-functions.php#L483 https://plugins.trac.wordpress.org/browser/wpdm-premium-packages/tags/7.2.1/src/Cart/CartItem.php#L96 https://plugins.trac.wordpress.org/browser/wpdm-premium-packages/tags/7.2.1/src/Cart/CartService.php#L328 https://plugins.trac.wordpress.org/browser/wpdm-premium-packages/tags/7.2.1/src/Order/OrderService.php#L1255 https://plugins.trac.wordpress.org/browser/wpdm-premium-packages/tags/7.2.1/templates/invoices/default/invoice.php#L167 https://plugins.trac.wordpress.org/changeset?reponame=&old=3708519%40wpdm-premium-packages&new=3708519%40wpdm-premium-packages			
CVE-2026-94573	7,2	The Repeater Fields for Elementor Forms plugin for Word-Press	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 2.2.7	https://plugins.trac.wordpress.org/browser/repeater-for-elementor/tags/2.2.7/fields/repeater_end.php#L237 https://plugins.trac.wordpress.org/browser/repeater-for-elementor/tags/2.2.7/fields/repeater_end.php#L309 https://plugins.trac.wordpress.org/browser/repeater-for-elementor/tags/2.2.7/fields/repeater_end.php#L317 https://plugins.trac.wordpress.org/browser/repeater-for-elementor/tags/2.2.7/libs/admin.js#L15 https://plugins.trac.wordpress.org/changeset?reponame=&old=3710785%40repeater-for-elementor&new=3710785%40repeater-for-elementor https://www.wordfence.com/threat-intel/vulnerabilities/id/ea28fc6c-50d6-406b-9205-3f1bec577644?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-2026-95864	7,2	The Themify Builder plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 7.8.1	https://plugins.trac.wordpress.org/browser/themify-builder/tags/7.8.1/classes/class-themify-builder-stylesheet.php#L160 https://plugins.trac.wordpress.org/browser/themify-builder/tags/7.8.1/classes/class-themify-builder-stylesheet.php#L317 https://plugins.trac.wordpress.org/browser/themify-builder/tags/7.8.1/classes/class-themify-builder-stylesheet.php#L514 https://plugins.trac.wordpress.org/browser/themify-builder/tags/7.8.1/themify/class-themify-enqueue.php#L1757 https://plugins.trac.wordpress.org/changeset?reponame=&old=3710320%40themify-builder&new=3710320%40themify-builder https://www.wordfence.com/threat-intel/vulnerabilities/id/fc021ee6-694a-426b-b399-8dd015fd99d2?source=cve			
CVE-2026-95866	7,2	The User Profile Builder – Beautiful User Registration Forms, User Profiles & User Role Editor plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 4.0.2	https://plugins.trac.wordpress.org/browser/profile-builder/tags/4.0.2/front-end/default-fields/avatar/avatar.php#L127 https://plugins.trac.wordpress.org/browser/profile-builder/tags/4.0.2/front-end/default-fields/avatar/avatar.php#L67 https://plugins.trac.wordpress.org/browser/profile-builder/tags/4.0.2/front-end/default-fields/upload/upload_helper_functions.php#L286 https://plugins.trac.wordpress.org/changeset?reponame=&old=3708665%40profile-builder&new=3708665%40profile-builder https://www.wordfence.com/threat-intel/vulnerabilities/id/68cef86f-3a6a-47c4-a092-de3bb40ac157?source=cve			
CVE-2026-96039	7,2	The BA Book Everything plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 1.8.27	https://plugins.trac.wordpress.org/browser/ba-book-everything/tags/1.8.27/includes/class-babe-html.php#L4300 https://plugins.trac.wordpress.org/browser/ba-book-everything/tags/1.8.27/includes/class-babe-order.php#L2405 https://plugins.trac.wordpress.org/browser/ba-book-everything/tags/1.8.27/includes/class-babe-order.php#L2522 https://plugins.trac.wordpress.org/browser/ba-book-everything/tags/1.8.27/includes/class-babe-order.php#L2599 https://plugins.trac.wordpress.org/browser/ba-book-everything/tags/1.8.27/includes/class-babe-order.php#L2653 https://plugins.trac.wordpress.org/changeset?reponame=&new=3709588%40ba-book-everything%2Ftrunk&old=3640320%40ba-book-everything%2Ftrunk			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-96568	7,2	The Restaurant Menu and Food Ordering plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 2.4.14	https://plugins.trac.wordpress.org/browser/mp-restaurant-menu/tags/2.4.14/classes/models/shop/class-order.php#L1497 https://plugins.trac.wordpress.org/browser/mp-restaurant-menu/tags/2.4.14/classes/models/shop/class-order.php#L465 https://plugins.trac.wordpress.org/browser/mp-restaurant-menu/tags/2.4.14/classes/models/shop/class-order.php#L725 https://plugins.trac.wordpress.org/browser/mp-restaurant-menu/tags/2.4.14/classes/models/shop/class-order.php#L727 https://plugins.trac.wordpress.org/browser/mp-restaurant-menu/tags/2.4.14/classes/models/shop/class-purchase.php#L494 https://plugins.trac.wordpress.org/changeset?reponame=&old=3709808%40mp-restaurant-menu&new=3709808%40mp-restaurant-menu			
CVE-2026-96752	7,2	The Zero Spam for WordPress plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 5.7.10	https://plugins.trac.wordpress.org/browser/zero-spam/tags/5.7.10/core/class-utilities.php#L65 https://plugins.trac.wordpress.org/browser/zero-spam/tags/5.7.10/includes/class-db.php#L442 https://plugins.trac.wordpress.org/browser/zero-spam/tags/5.7.10/includes/templates/admin-modal-details.php#L200 https://plugins.trac.wordpress.org/browser/zero-spam/tags/5.7.10/modules/contactform7/class-contactform7.php#L85 https://plugins.trac.wordpress.org/changeset?reponame=&old=3709762%40zero-spam&new=3709762%40zero-spam https://www.wordfence.com/threat-intel/vulnerabilities/id/01540d78-ae46-4556-9a7f-3f8b8dbbcbcd7?source=cve			
CVE-2026-82164	7,1	Dell Trusted Device Client, versions	Incorrect Permission Assignment for Critical Resource	versions prior to 8.1.359.0	https://www.dell.com/support/kbdoc/en-us/000506918/dsa-2026-408-security-update-for-dell-trusted-device-client-for-an-incorrect-permission-assignment-for-critical-resource-vulnerability	none	no	total
CVE-2026-97731	7,1	MinIO; the client-supplied X-Amz-SignedHeaders list	Improper Verification of Cryptographic Signature	through 7aac2a2; before 1233254	https://github.com/pgstv/silo/commit/1233254309b15571f101b2b26d531951ceaeef1e https://silo.pgstv.com/about/security-advisories/#sn-2026-011			

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-2026-5430 WSO2 Multiple Products Path Traversal Vulnerability ▪ CVE-2026-71362 Adobe Commerce and Magento Incorrect Authorization Vulnerability	https://cisa.gov/news-events/alerts/2026/09/24/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 steal \$351.6 million in Bitget crypto exchange hack	https://bleepingcomputer.com/news/security/hackers-steal-3516-million-in-bitget-crypto-exchange-hack
Duelbits Confirms \$7 Million Hot-Wallet Hack, forcing Systems offline	https://cybersecuritynews.com/duelbits-7-million-hack
Hackers Exploited Ethereum Bridge Contract to Drain Full Balance from Payy Network	https://cybersecuritynews.com/payy-ethereum-bridge-contract-drain
Autonomous AI Hacks Raise Thorny Questions of Legal Accountability	https://securityweek.com/autonomous-ai-hacks-raise-thorny-questions-of-legal-accountability
SectopRAT Returns, Hiding Inside a Legitimate Application	https://darkreading.com/cyberattacks-data-breaches/sectopratt-returns-hiding-inside-legitimate-application
SCOUTz Prospect Intelligence Platform Launches for MSPs with 30-Day Beta	https://cybersecuritynews.com/scoutz-prospect-intelligence-platform-launches-for-msps-with-30-day-beta
ThreatsDay: AI Search Poisoning, AI Coding Tool Leaking Repos, One-Click Code Execution and 13 More Stories	https://thehackernews.com/2026/09/threatsday-ai-search-poisoning-ai.html
Researchers Found a New Way to Break RSA that Doesn't Require Factoring the Key	https://cybersecuritynews.com/new-way-to-break-rsa
Exposed GitLab project email addresses let attackers push code	https://bleepingcomputer.com/news/security/exposed-gitlab-project-email-addresses-let-attackers-push-code
Kontext Security Emerges With \$4 Million for AI Agent Runtime Controls	https://securityweek.com/kontext-security-emerges-with-4-million-for-ai-agent-runtime-controls
Prompt-Injection Bug Hits \$4B Agentic AI App 'Manus'	https://darkreading.com/application-security/prompt-injection-bug-agentic-ai-app-manus
CISA Charts New	https://infosecurity-magazine.com/news/cisa-quality-era-global-cve-program
Windows 11 KB5124010 update released with 46 changes and fixes	https://bleepingcomputer.com/news/microsoft/windows-11-kb5124010-update-released-with-46-changes-and-fixes
Island Raises \$400 Million at \$6.4 Billion Valuation	https://securityweek.com/island-raises-400-million-at-6-4-billion-valuation

Microsoft Rebuilds the SOC with AI Agents, SIEM Integration and Machine-Speed Defense	https://cybersecuritynews.com/microsoft-rebuilds-the-soc
UK Government Shifts to Service-Led Cyber Governance After Audit	https://infosecurity-magazine.com/news/uk-government-service-led-cyber
OpenAI Agent Hacks Australian Medicare Portal	https://infosecurity-magazine.com/news/openai-hacks-australian-medicare
New Android Banking Trojan Uses AI-Built Overlays to Steal Users' Banking PINs	https://cybersecuritynews.com/android-banking-trojan
Over 75% of Organizations Experience Microsoft 365 Governance Issues	https://infosecurity-magazine.com/news/75-organizations-microsoft-365
Data Overtakes Skills as Top Threat Hunting Challenge, SANS Study Find	https://infosecurity-magazine.com/news/data-top-bottleneck-barrier-threat

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
Bitget Hot Wallet Hacked - Attackers Stole \$351.6 Million From Hot Wallets	https://cybersecuritynews.com/bitget-hot-wallet-hacked
Astrana Health Data Breach Impacts Private, Confidential Information	https://securityweek.com/astrana-health-data-breach-impacts-private-confidential-information
OpenAI hacked Australian Medicare govt site, probed data providers	https://bleepingcomputer.com/news/security/openai-hacked-australian-medicare-govt-site-probed-data-providers
OpenAI Agent Hacked Australian Government Medicare Portal in World's First Rogue AI Breach	https://cybersecuritynews.com/openai-agent-hacked-australian-portal

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
Salesforce Indirect Prompt Injection Vulnerability Enables 0-click Data Exfiltration	https://cybersecuritynews.com/salesforce-salesbleed-vulnerability
Roundcube Webmail Vulnerability in Attackers' Crosshairs	https://securityweek.com/roundcube-webmail-vulnerability-in-attackers-crosshairs
WSO2 and Adobe Commerce Flaws Exploited in Attacks, Added to CISA KEV	https://thehackernews.com/2026/09/wso2-and-adobe-commerce-flaws-exploited.html
Cloudflare Containers Vulnerability Could Leak Data Between Customer Workloads	https://cybersecuritynews.com/cloudflare-containers-vulnerability

OpenAI Agents Probed Websites for Vulnerabilities While Fetching Public Data	https://securityweek.com/openai-agents-probed-websites-for-vulnerabilities-while-fetching-public-data
Hackers now exploit critical Roundcube flaw in code injection attacks	https://bleepingcomputer.com/news/security/critical-roundcube-flaw-now-actively-exploited-in-code-injection-attacks
Roundcube Webmail SQL Injection Vulnerability Exploited in the Wild	https://cybersecuritynews.com/roundcube-webmail-vulnerability-exploited
Hackers Exploit Critical Check Point VPN Flaws to Gain Remote Access Without Login	https://cybersecuritynews.com/hackers-exploit-critical-check-point-vpn-flaws
Critical WordPress Vulnerability Exploited Immediately After Disclosure	https://securityweek.com/critical-wordpress-vulnerability-exploited-immediately-after-disclosure
Attackers Exploit WordPress CVE-2026-87902 Within Hours of Disclosure	https://thehackernews.com/2026/09/attackers-exploit-wordpress-cve-2026.html
Check Point warns of hackers exploiting Security Gateway VPN RCE flaw	https://bleepingcomputer.com/news/security/check-point-warns-of-hackers-exploiting-security-gateway-vpn-rce-flaw
Hackers start exploiting critical WordPress flaw for code execution	https://bleepingcomputer.com/news/security/hackers-start-exploiting-critical-wordpress-flaw-for-code-execution
GitLab Email Feature Vulnerability Lets Attackers Push Code Into Private Repositories	https://cybersecuritynews.com/gitlab-email-private-repository-flaw
AWS Lambda Flaw Lets Attackers Bypass IAM Permissions and Access Cloud Services	https://cybersecuritynews.com/aws-lambda-flaw
Critical NEXT.JS Flaw Enables RCE Attacks Via Weaponized SVG File	https://cybersecuritynews.com/critical-next-js-flaw-allows-remote-code-execution
New cPanel Flaw Lets a Hosting Account Run Code as Root, Take Full Server Control	https://thehackernews.com/2026/09/new-cpanel-flaw-lets-hosting-account_0272795595.html
Arista Urges Immediate Patching of Exploited VCO Zero-Day	https://securityweek.com/arista-urges-immediate-patching-of-exploited-vco-zero-day
Critical F5 BIG-IP Vulnerability Exploited as Zero-Day	https://securityweek.com/critical-f5-big-ip-vulnerability-exploited-as-zero-day
Critical Next.js ImageResponse Flaw Can Lead to Server Code Execution via Crafted SVG Input	https://thehackernews.com/2026/09/critical-nextjs-imageresponse-flaw-can.html

Patches / Updates / Fixes

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

Σύντομη περιγραφή / Τίτλος	URL
Cloudflare Fixes Flaw That Let One Container Read Another Customer's Leftover Disk Data	https://thehackernews.com/2026/09/cloudflare-fixes-flaw-that-let-one.html
Unpatched OnePlus Flaws Let Installed Android Apps Gain Root Without Permissions	https://thehackernews.com/2026/09/unpatched-oneplus-flaws-let-installed.html
SolarWinds Patches Critical RCE Flaws in Observability Self-Hosted	https://securityweek.com/solarwinds-patches-critical-rce-flaws-in-observability-self-hosted
Microsoft fixes bug that broke Windows File History backup feature	https://bleepingcomputer.com/news/microsoft/microsoft-fixes-windows-backup-feature-broken-by-september-updates
Apache Tomcat Update Fixes WebSocket and HTTP/2 Flaws Affecting Server Security	https://cybersecuritynews.com/apache-tomcat-update

Arista patches actively exploited VeloCloud Orchestrator zero-day	https://bleepingcomputer.com/news/security/arista-patches-actively-exploited-velocloud-orchestrator-zero-day
Adobe Patches Critical Flaws in Connect, AEM Forms	https://securityweek.com/adobe-patches-critical-flaws-in-connect-aem-forms
Exploit Released for Unpatched Ubuntu Linux Flaw Enabling Host-Root Container Escape	https://thehackernews.com/2026/09/exploit-released-for-unpatched-ubuntu.html
Chrome 154 Patches 108 Vulnerabilities	https://securityweek.com/chrome-154-patches-108-vulnerabilities
F5 Patches Critical BIG-IP APM Zero-Day Exploited for Unauthenticated RCE on OAuth Servers	https://thehackernews.com/2026/09/f5-patches-critical-big-ip-apm-zero-day.html
Chrome Patches 108 Vulnerabilities Including Critical Flaws that Enable Code Execution Attacks	https://cybersecuritynews.com/chrome-patches-108-vulnerabilities
F5 patches BIG-IP APM zero-day flaw exploited in RCE attacks	https://bleepingcomputer.com/news/security/f5-warns-of-big-ip-apm-remote-code-execution-zero-day-exploited-in-attacks
Check Point Patches Exploited Management Server Zero-Day	https://securityweek.com/check-point-patches-exploited-management-server-zero-day

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
Researchers Identify AliExpress Phishing Domains Before Registration	https://infosecurity-magazine.com/news/aliexpress-phishing-flagged-early
New MacSync Malware Turns macOS Apps Into Tools for Crypto and Password Theft	https://cybersecuritynews.com/new-macsync-malware
'Salesbleed' Exploits Salesforce Agents to Enable Slack Phishing	https://darkreading.com/application-security/salesbleed-exploits-salesforce-agents-slack-phishing
MacSync malware uses public iCloud calendars to deliver new payloads	https://bleepingcomputer.com/news/security/macsync-malware-uses-public-icloud-calendars-to-deliver-new-payloads
New Carbonato malware uses AI agents to hijack exposed Docker hosts	https://bleepingcomputer.com/news/security/new-carbonato-malware-uses-ai-agents-to-hijack-exposed-docker-hosts
Emerging Ransomware Gang Uses Backup Destruction Threats	https://infosecurity-magazine.com/news/ransomware-gang-uses-backup
Fake PDF Files Hide Konni Malware Campaign Targeting Ukraine Organizations	https://cybersecuritynews.com/konni-malware-campaign
AI-Powered Campaign Targets Hundreds of Online Retailers	https://securityweek.com/ai-powered-campaign-targets-hundreds-of-online-retailers
AvisLoader Windows Malware That Learned to Survive Even After Its Servers Are Taken Down	https://cybersecuritynews.com/avisloader-windows-malware
CISA: Ransomware gangs now exploiting critical TeamCity flaw	https://bleepingcomputer.com/news/security/cisa-ransomware-gangs-now-exploiting-critical-teamcity-flaw
New Galago Ransomware Operation Emerges With Links to Panzer Group	https://cybersecuritynews.com/new-galago-ransomware
New RemControl Android banking malware targets users in Europe and Canada	https://bleepingcomputer.com/news/security/new-remcontrol-android-banking-malware-targets-users-in-europe-and-canada
The Visibility Gap in Phishing Detection: Where Sandboxing Makes a Difference	https://cybersecuritynews.com/the-visibility-gap-in-phishing-detection-where-sandboxing-makes-a-difference

Attackers Manipulate AI in Mass Disinformation, Phishing Campaign	https://darkreading.com/threat-intelligence/attackers-manipulate-ai-chatbots-mass-disinformation-phishing-campaign
Windows Botnet x47.c Offers AI API Draining, 18 Attack Methods	https://infosecurity-magazine.com/news/x47c-botnet-ai-api-draining-18
Ransomware Attacks Reach Record High for 2026	https://infosecurity-magazine.com/news/ransomware-attacks-reach-record
Chinese Hackers Exploit Chrome-Windows Zero-Day Chain to Deploy CLEANGULP Malware	https://thehackernews.com/2026/09/chinese-hackers-exploit-chrome-windows.html

Guides / Tools

Παρουσιάζονται τεχνικοί οδηγοί και εργαλεία που μπορούν να βοηθήσουν στην παρακολούθηση, ανάλυση ή ενίσχυση της ασφάλειας συστημάτων. Είτε πρόκειται για open source projects είτε για νέες τεχνικές, η ενότητα αυτή λειτουργεί ως πόρος για πρακτικές λύσεις στην καθημερινή δουλειά των επαγγελματιών ασφάλειας.

Σύντομη περιγραφή / Τίτλος	URL
OT Security Guidance: NIST Drafts Updated Guide, CISA/FBI Advise on ICS Integrators	https://securityweek.com/ot-security-guidance-nist-drafts-updated-guide-cisa-fbi-advise-on-ics-integrators
Begin at the End: How to Enable Agentic Remediation	https://securityweek.com/begin-at-the-end-how-to-enable-agentic-remediation

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 23/09/2026–25/09/2026, 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/