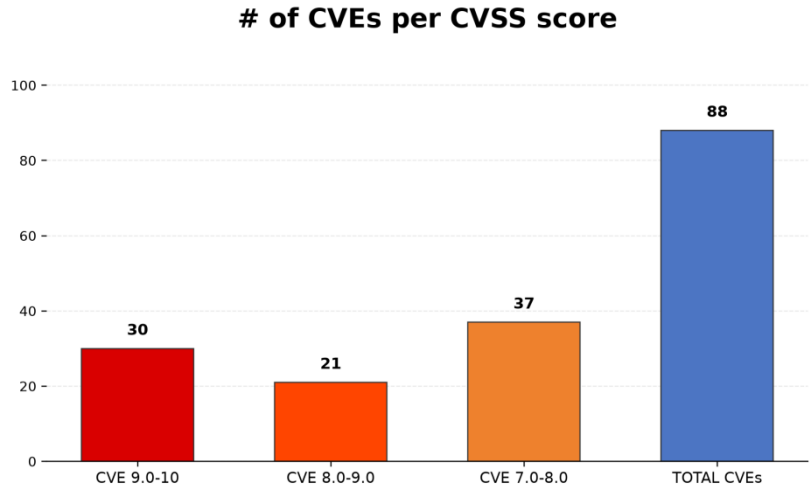
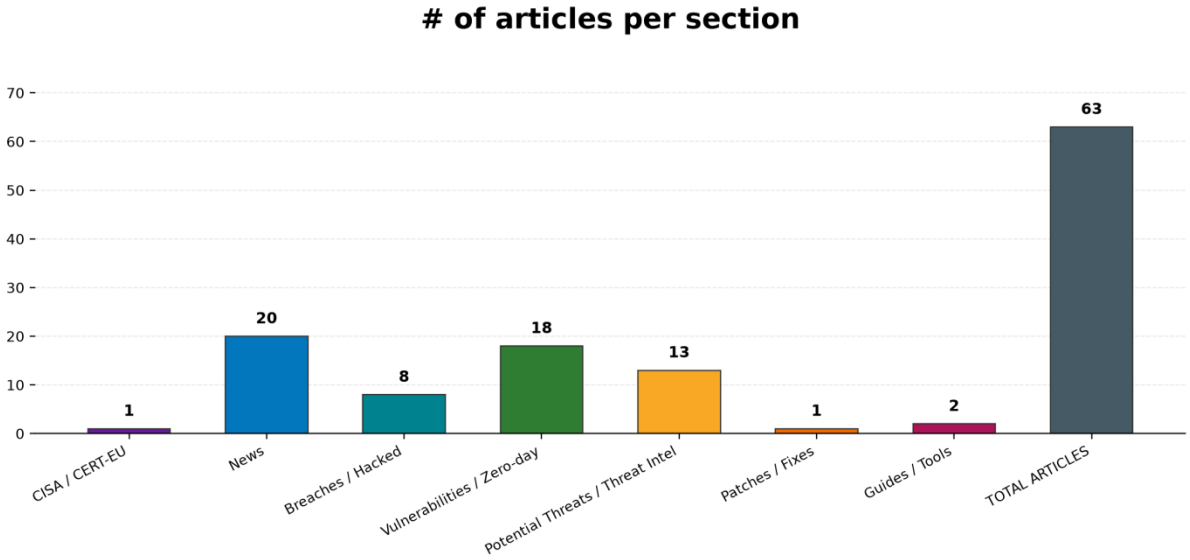
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 15/08/2026 - 18/08/2026





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-2026-72407	10,0	Linux		fd0dd796576e1a560e1441e665810129f0a82be0 prior to e2087447f562692ff0cd08a0554d8d4ad083aa5c; fd0dd796576e1a560e1441e665810129f0a82be0 prior to cbb0d30a1ad6fc9439b1dc9b4f5a7a9140d3b11f; 7.0	https://git.kernel.org/stable/c/cbb0d30a1ad6fc9439b1dc9b4f5a7a9140d3b11f https://git.kernel.org/stable/c/e2087447f562692ff0cd08a0554d8d4ad083aa5c			
CVE-2026-72408	10,0	geneve_gro_complete() on gs->gro_hint geneve_gro_receive() reads the GRO hint		fd0dd796576e1a560e1441e665810129f0a82be0 prior to 49c2e7c0a69999a75ef5eaebe1559a20d0b3c15a; fd0dd796576e1a560e1441e665810129f0a82be0 prior to 2651c174445884ac9e85622aeade9c1f7b98d8e5; 7.0	https://git.kernel.org/stable/c/2651c174445884ac9e85622aeade9c1f7b98d8e5 https://git.kernel.org/stable/c/49c2e7c0a69999a75ef5eaebe1559a20d0b3c15a			
CVE-2026-74475	10,0	route_shortcircuit() The neighbour hardware address n->ha		e4f67addf158f98f8197e08974966b18480dc751 prior to d08e8ac13f2e228cc7fc3c70b5ebe71557b624a0; e4f67addf158f98f8197e08974966b18480dc751 prior to ec341bb76d77b4c2948764375ee6bfeef4bb41c3; e4f67addf158f98f8197e08974966b18480dc751 prior to ff89415d34c3ab9f5312316423122e664ed3524f; e4f67addf158f98f8197e08974966b18480dc751 prior to 05f2987f73daa05333fd713d05546142f9f7c5f0; e4f67addf158f98f8197e08974966b18480dc751 prior to 8eca411347e1d38964f9ed2c8d3b6ab0e7e4473d; 3.8	https://git.kernel.org/stable/c/05f2987f73daa05333fd713d05546142f9f7c5f0 https://git.kernel.org/stable/c/8eca411347e1d38964f9ed2c8d3b6ab0e7e4473d https://git.kernel.org/stable/c/d08e8ac13f2e228cc7fc3c70b5ebe71557b624a0 https://git.kernel.org/stable/c/ec341bb76d77b4c2948764375ee6bfeef4bb41c3 https://git.kernel.org/stable/c/ff89415d34c3ab9f5312316423122e664ed3524f			
CVE-2026-47686	9,9	vm2	Protection Mechanism Failure	Prior to 3.11.6	https://github.com/patriksimek/vm2/commit/7e3faaf550f4ab975bf4cdde183fcec49b056d8e https://github.com/patriksimek/vm2/releases/tag/3.11.6 https://github.com/patriksimek/vm2/security/advisories/GHSA-m283-3h24-438v			
CVE-2024-13784	9,8	The Contact Form, Survey, Quiz & Popup Form Builder – ARForms plugin for WordPress	Deserialization of Untrusted Data	up to, and including, 1.8.5	https://wordpress.org/plugins/arforms-form-builder/ https://www.wordfence.com/threat-intel/vulnerabilities/id/5e0116d6-91c3-4212-9c68-6b706ab09768?source=cve	none	yes	total
CVE-2026-15303	9,8	The 6Storage Rentals plugin for WordPress	Improper Authentication	up to, and including, 2.27.0.	https://plugins.trac.wordpress.org/browser/6storage-rentals/tags/2.27.0/inc/Base/Six_Storage_DashboardController.php#L14 https://plugins.trac.wordpress.org/browser/6storage-rentals/tags/2.27.0/inc/Base/Six_Storage_DashboardController.php#L3834 https://plugins.trac.wordpress.org/browser/6storage-rentals/tags/2.27.0/inc/Base/Six_Storage_DashboardController.php#L3905 https://www.wordfence.com/threat-intel/vulnerabilities/id/94e987be-bdfc-4691-b250-2b7d7249df0a?source=cve	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-2026-15341	9,8	The User Session Synchronizer plugin for WordPress	Improper Authentication	up to, and including, 1.4.0.	https://plugins.trac.wordpress.org/browser/user-session-synchronizer/tags/1.4.0/includes/class-user-session-synchronizer.php#L117 https://plugins.trac.wordpress.org/browser/user-session-synchronizer/tags/1.4.0/includes/class-user-session-synchronizer.php#L286 https://plugins.trac.wordpress.org/browser/user-session-synchronizer/tags/1.4.0/includes/class-user-session-synchronizer.php#L310 https://plugins.trac.wordpress.org/browser/user-session-synchronizer/tags/1.4.0/includes/class-user-session-synchronizer.php#L422 https://plugins.trac.wordpress.org/browser/user-session-synchronizer/tags/1.4.0/includes/class-user-session-synchronizer.php#L598 https://plugins.trac.wordpress.org/browser/user-session-synchronizer/tags/1.4.0/includes/class-user-session-synchronizer.php#L631	none	yes	total
CVE-2026-15748	9,8	The Forminator Forms plugin for WordPress; all	Unrestricted Upload of File with Dangerous Type	up to, and including, 1.56.1	https://plugins.trac.wordpress.org/browser/forminator/tags/1.55.1/admin/classes/class-admin-ajax.php#L1196 https://plugins.trac.wordpress.org/browser/forminator/tags/1.55.1/library/abstracts/abstract-class-field.php#L2308 https://plugins.trac.wordpress.org/browser/forminator/tags/1.55.1/library/fields/upload.php#L552 https://plugins.trac.wordpress.org/browser/forminator/tags/1.55.1/library/helpers/helper-fields.php#L3425 https://plugins.trac.wordpress.org/browser/forminator/tags/1.55.1/library/modules/custom-forms/front/front-action.php#L2767 https://plugins.trac.wordpress.org/browser/forminator/tags/1.55.1/library/modules/custom-forms/front/front-action.php#L738			
CVE-2026-15826	9,8	The User Profile Builder plugin for WordPress	Incorrect Type Conversion or Cast	up to, and including, 3.16.4.	https://plugins.trac.wordpress.org/browser/profile-builder/tags/3.16.4/features/functions.php#L1481 https://plugins.trac.wordpress.org/browser/profile-builder/tags/3.16.4/front-end/class-formbuilder.php#L262 https://plugins.trac.wordpress.org/browser/profile-builder/tags/3.16.4/front-end/class-formbuilder.php#L364 https://plugins.trac.wordpress.org/browser/profile-builder/tags/3.16.4/front-end/class-formbuilder.php#L742 https://plugins.trac.wordpress.org/browser/profile-builder/tags/3.16.4/front-end/class-formbuilder.php#L945 https://plugins.trac.wordpress.org/browser/profile-builder/tags/3.16.4/front-end/default-fields/username/username.php#L28	none	yes	total
CVE-2026-19349	9,8	Lemonldap::NG::Portal	Authentication Bypass by Primary Weakness; Function Call with Incorrectly Specified Arguments	before 2.16.9; before 2.21.5; before 2.23.3	https://gitlab.ow2.org/lemonldap-ng/lemonldap-ng/-/releases/v2.16.9 https://gitlab.ow2.org/lemonldap-ng/lemonldap-ng/-/releases/v2.21.5 https://gitlab.ow2.org/lemonldap-ng/lemonldap-ng/-/releases/v2.23.3 http://www.openwall.com/lists/oss-security/2026/08/16/2	none	yes	total
CVE-2026-19598	9,8	The Pods – Custom Content Types and Fields plugin for WordPress	Incorrect Authorization	up to, and including, 3.3.9.	https://plugins.trac.wordpress.org/browser/pods/tags/3.3.9/includes/general.php#L400 https://www.wordfence.com/threat-intel/vulnerabilities/id/3628032a-3121-45a7-8a78-cfcd8ba6af2f?source=cve	none	yes	total
CVE-2026-72098	9,8	FEC calculation There's a buffer overflow in dm-verity-fec: if (neras && *neras <= v->fec->roots) fio->erasures[(*neras)++] = i		a739ff3f543afbb4a041c16cd0182c8e8d366e70 prior to 5488d3a69d205e28f74f18857b853aa12e778e66; a739ff3f543afbb4a041c16cd0182c8e8d366e70 prior to f7990c2b0f08b8841fcd2652d1d7002f5994a7a7; a739ff3f543afbb4a041c16cd0182c8e8d366e70 prior to 31d6e6c0ba8d5a7bd59660035a089307100c5e8e; 4.5	https://git.kernel.org/stable/c/31d6e6c0ba8d5a7bd59660035a089307100c5e8e https://git.kernel.org/stable/c/5488d3a69d205e28f74f18857b853aa12e778e66 https://git.kernel.org/stable/c/f7990c2b0f08b8841fcd2652d1d7002f5994a7a7			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-72192	9,8	indx_insert_into_root		82cae269cfa953032fbb8980a7d554d60fb00b17 prior to 0af83b8155cc848e9f5d2c36e20a70d024214649; 82cae269cfa953032fbb8980a7d554d60fb00b17 prior to cb3161deebcaf8d36d3115abf452c633f2180fc1; 82cae269cfa953032fbb8980a7d554d60fb00b17 prior to 53c5f3b2da3774b41534728aba295c098c9efa19; 82cae269cfa953032fbb8980a7d554d60fb00b17 prior to 194b00c99ba971fa7cf6acd747a36032c6de54eb; 82cae269cfa953032fbb8980a7d554d60fb00b17 prior to aaa1f956c0fc41089a4a534da7df91552a08a47c; 82cae269cfa953032fbb8980a7d554d60fb00b17 prior to d240f5f9d036b8180224954d9873f172b6be4dd8; 82cae269cfa953032fbb8980a7d554d60fb00b17 prior to 9b6926ac9c970ae0b2c2fe6289b16e9aa10b6a67; 5.15	https://git.kernel.org/stable/c/0af83b8155cc848e9f5d2c36e20a70d024214649 https://git.kernel.org/stable/c/194b00c99ba971fa7cf6acd747a36032c6de54eb https://git.kernel.org/stable/c/53c5f3b2da3774b41534728aba295c098c9efa19 https://git.kernel.org/stable/c/9b6926ac9c970ae0b2c2fe6289b16e9aa10b6a67 https://git.kernel.org/stable/c/aaa1f956c0fc41089a4a534da7df91552a08a47c https://git.kernel.org/stable/c/cb3161deebcaf8d36d3115abf452c633f2180fc1			
CVE-2026-72249	9,8	this direction when pushing IPIP header When pushing the IPIP header, the route of the other direction		d30301ba4b07ac92eb38353a111833b009003170 prior to ecb78fbb03d3f86e2e93767875e273308086a424; d30301ba4b07ac92eb38353a111833b009003170 prior to c328b90c17fc5fa7786503695152880b2afb9326; 6.19	https://git.kernel.org/stable/c/c328b90c17fc5fa7786503695152880b2afb9326 https://git.kernel.org/stable/c/ecb78fbb03d3f86e2e93767875e273308086a424			
CVE-2026-72319	9,8	ICMP errors		f2edb9f7706dcb2c0d9a362b2ba849efe3a97f5e prior to 19657b3a17b774ae4e2f2635b5ae8638c9344a40; f2edb9f7706dcb2c0d9a362b2ba849efe3a97f5e prior to dac813101914c21219ac221a60a31a11bc90e7ec; f2edb9f7706dcb2c0d9a362b2ba849efe3a97f5e prior to dd22f74a09e25ca298ced0a3763ef353242cb78d; f2edb9f7706dcb2c0d9a362b2ba849efe3a97f5e prior to 9bc9b95aee2b2e3f1301a16a67ee504960402875; f2edb9f7706dcb2c0d9a362b2ba849efe3a97f5e prior to a735f9964a3d9ed97daf9b08507f8b5bcafe6326; f2edb9f7706dcb2c0d9a362b2ba849efe3a97f5e prior to 8f48cfe657409fb5c7ba0521b14da6d47546d9cf; f2edb9f7706dcb2c0d9a362b2ba849efe3a97f5e prior to 92185d6f7819bc558939ae83de7b1abe90e3b5c2; f2edb9f7706dcb2c0d9a362b2ba849efe3a97f5e prior to 3f7a535ff0fa627a0132803e4c2f903ceffcbc1c; 3.7	https://git.kernel.org/stable/c/19657b3a17b774ae4e2f2635b5ae8638c9344a40 https://git.kernel.org/stable/c/3f7a535ff0fa627a0132803e4c2f903ceffcbc1c https://git.kernel.org/stable/c/8f48cfe657409fb5c7ba0521b14da6d47546d9cf https://git.kernel.org/stable/c/92185d6f7819bc558939ae83de7b1abe90e3b5c2 https://git.kernel.org/stable/c/9bc9b95aee2b2e3f1301a16a67ee504960402875 https://git.kernel.org/stable/c/a735f9964a3d9ed97daf9b08507f8b5bcafe6326			
CVE-2026-72463	9,8	xfrm async resumption xfrm async resumption hold skb->dev refcnt until after transport_finish		1c428b03840094410c5fb6a5db30640486bbbfcb prior to 63a30015199912bd5055bead8001b1ae68a67cdb; 1c428b03840094410c5fb6a5db30640486bbbfcb prior to 8045c0df98d4f14c54e5cb875f1c9c0ce89fe4ff; 4236c30b437b80f673b9e08c8fae38b8d471ac9e; 0f451b43c88bf2b9c038b414be580efee42e031b; 5002beda5cac69d522dc54da0d5d463ed9c963d2; 6.12.94 prior to 6.13; 6.18.23 prior to 6.19; 6.19.13 prior to 6.20; 7.0	https://git.kernel.org/stable/c/63a30015199912bd5055bead8001b1ae68a67cdb https://git.kernel.org/stable/c/8045c0df98d4f14c54e5cb875f1c9c0ce89fe4ff			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-74255	9,8	tipc_l2_send_msg() Syzbot reported a slab-use-after-free in ipvlan_hard_header() when called from tipc_l2_send_msg()		282b3a056225b35024246f63feb91d769d714dad prior to 609ced2301be1df7e7ed2ef47d1d916674e6ba3b; 282b3a056225b35024246f63feb91d769d714dad prior to 71aafa16d79b107b33837f60b6cbc7d0cb8c5708; 282b3a056225b35024246f63feb91d769d714dad prior to f4002f1c669cc02e3763f479fc25ff1dfa9e2420; 282b3a056225b35024246f63feb91d769d714dad prior to 50ff092633b06382e5091dd5b093ce943d4ac2f9; 282b3a056225b35024246f63feb91d769d714dad prior to aef12b5ce793dea6b3a97a58fd0f946000ae8945; 282b3a056225b35024246f63feb91d769d714dad prior to 0d8a12d7143126afdf9fbe2e3d438650dd6603ed; 282b3a056225b35024246f63feb91d769d714dad prior to 35e0297a93c3c34a3924eeef816c03504e3ab5c5; 282b3a056225b35024246f63feb91d769d714dad prior to f4c3d89fc986b0da196ddfc6cfe0ea5d5d08bec6; 4.4	https://git.kernel.org/stable/c/0d8a12d7143126afdf9fbe2e3d438650dd6603ed https://git.kernel.org/stable/c/35e0297a93c3c34a3924eeef816c03504e3ab5c5 https://git.kernel.org/stable/c/50ff092633b06382e5091dd5b093ce943d4ac2f9 https://git.kernel.org/stable/c/609ced2301be1df7e7ed2ef47d1d916674e6ba3b https://git.kernel.org/stable/c/71aafa16d79b107b33837f60b6cbc7d0cb8c5708 https://git.kernel.org/stable/c/aef12b5ce793dea6b3a97a58fd0f946000ae8945			
CVE-2026-74394	9,8	immediate data length check imm_buf->len		5dabcd0456d7ee17c2c7a17d7c2305444d2b9639 prior to c82c860f8c8e4f4f454c9f14d0ad0c0466965f7d; 5dabcd0456d7ee17c2c7a17d7c2305444d2b9639 prior to 3efa5301137140a3ca3677a9098c0a93a0acfd49; 5dabcd0456d7ee17c2c7a17d7c2305444d2b9639 prior to 067b9556eeb007f28b7c2033b4dcde5b6d88418f; 5dabcd0456d7ee17c2c7a17d7c2305444d2b9639 prior to dcf7a986f377cce0749ed53f1d64195fbd5fdf91; 5dabcd0456d7ee17c2c7a17d7c2305444d2b9639 prior to 07dec3f6dcb6c6cc891162d252b800eb0e6d5e8e; 5dabcd0456d7ee17c2c7a17d7c2305444d2b9639 prior to 65572fbd86033ae2370125593d59b8be34253aaf; 5dabcd0456d7ee17c2c7a17d7c2305444d2b9639 prior to 72497172a4799119a0282a5eb5e2b8ddcc821921; 5dabcd0456d7ee17c2c7a17d7c2305444d2b9639 prior to eb4ecdf631fe00e8020bf461503cb9b7017ed796; 5.0	https://git.kernel.org/stable/c/067b9556eeb007f28b7c2033b4dcde5b6d88418f https://git.kernel.org/stable/c/07dec3f6dcb6c6cc891162d252b800eb0e6d5e8e https://git.kernel.org/stable/c/3efa5301137140a3ca3677a9098c0a93a0acfd49 https://git.kernel.org/stable/c/65572fbd86033ae2370125593d59b8be34253aaf https://git.kernel.org/stable/c/72497172a4799119a0282a5eb5e2b8ddcc821921 https://git.kernel.org/stable/c/c82c860f8c8e4f4f454c9f14d0ad0c0466965f7d			
CVE-2026-74428	9,8	rxrpc_recvmsg() Fix a double unlock in rxrpc_recvmsg() when dealing with OOB messages		5800b1cf3fd8ccab752a101865be1e76dac33142 prior to 8cd8cf3052fff9a4b86b25734f610e4af03786d3; 5800b1cf3fd8ccab752a101865be1e76dac33142 prior to 1297ae6aeebc3863cb437e42a1bc4cd6173e43d9; 5800b1cf3fd8ccab752a101865be1e76dac33142 prior to a2f299b4d5510147fa8629a6aba2869bbcc88aea; 6.16	https://git.kernel.org/stable/c/1297ae6aeebc3863cb437e42a1bc4cd6173e43d9 https://git.kernel.org/stable/c/8cd8cf3052fff9a4b86b25734f610e4af03786d3 https://git.kernel.org/stable/c/a2f299b4d5510147fa8629a6aba2869bbcc88aea			
CVE-2026-74495	9,8	TX DMA error cleanup If an error		c1fa347f20f17f14a4a1575727fa24340e8a9117 prior to 31089f4eab42e0fc248ec80c26f9b0bad59ba4cc; c1fa347f20f17f14a4a1575727fa24340e8a9117 prior to bc25d56c03e41c10bc4b40e99ca5d7b941675c04; c1fa347f20f17f14a4a1575727fa24340e8a9117 prior to 845a9cdd9b03b7b6fa8de3ee80579780350a7f65; c1fa347f20f17f14a4a1575727fa24340e8a9117 prior to df07003b5a6c6c9fce60d765d6a3da815a74c41c; c1fa347f20f17f14a4a1575727fa24340e8a9117 prior to 0565052b7e2f436b7f1541f4849da96dc0aa7a0e; 2.6.33	https://git.kernel.org/stable/c/0565052b7e2f436b7f1541f4849da96dc0aa7a0e https://git.kernel.org/stable/c/31089f4eab42e0fc248ec80c26f9b0bad59ba4cc https://git.kernel.org/stable/c/845a9cdd9b03b7b6fa8de3ee80579780350a7f65 https://git.kernel.org/stable/c/bc25d56c03e41c10bc4b40e99ca5d7b941675c04 https://git.kernel.org/stable/c/df07003b5a6c6c9fce60d765d6a3da815a74c41c			
CVE-2026-74872	9,8	openssl_encrypt versions	Untrusted Search Path	versions before 1.4.0	https://github.com/jahlives/openssl_encrypt/security/advisories/GHSA-j48g-4c78-rhf9 https://www.vulncheck.com/advisories/openssl-encrypt-before-arbitrary-code-execution-via-whirlpool			
CVE-2026-74894	9,8	openssl_encrypt	Improper Authentication	before 1.4.0	https://github.com/jahlives/openssl_encrypt/security/advisories/GHSA-4g2c-wpqj-49w8 https://www.vulncheck.com/advisories/openssl-encrypt-before-authentication-bypass-via-bearer-token	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-2026-19478	9,4	GitLab CE/EE affecting all	Improper Control of Generation of Code ('Code Injection')	18; before 18.11.11, 19.0; before 19.0.8, 19.1; before 19.1.6; before 19.2.4	https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-2-4-released/ https://gitlab.com/gitlab-org/gitlab/-/work_items/611377 https://hackerone.com/reports/3926431	none	yes	partial
CVE-2026-72291	9,3	try_get_locked_pte() Fix an unlikely race in try_get_locked_pte(), which		89fa757931dc0bcd64ef22b28d1d5ad00c5d02f4 prior to ce587046baacdeb774b7756ab29b3f594e429004; 89fa757931dc0bcd64ef22b28d1d5ad00c5d02f4 prior to 5670b7f927f8d98685f3f5873dbf9f8d7a5a63f3; 7.1	https://git.kernel.org/stable/c/5670b7f927f8d98685f3f5873dbf9f8d7a5a63f3 https://git.kernel.org/stable/c/ce587046baacdeb774b7756ab29b3f594e429004			
CVE-2026-14524	9,1	The ProSolution WP Client plugin for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	up to, and including, 2.0.8.	https://plugins.trac.wordpress.org/browser/prosolution-wp-client/tags/2.0.3/includes/class-prosolwpclient.php#L260 https://plugins.trac.wordpress.org/browser/prosolution-wp-client/tags/2.0.3/public/class-prosolwpclient-public.php#L1135 https://plugins.trac.wordpress.org/browser/prosolution-wp-client/tags/2.0.3/public/class-prosolwpclient-public.php#L1256 https://plugins.trac.wordpress.org/changeset?reponame=&old=3634993%40prosolution-wp-client&new=3634993%40prosolution-wp-client https://www.wordfence.com/threat-intel/vulnerabilities/id/4e9698f0-b228-4f4e-838b-c0c0a193d675?source=cve	none	yes	partial
CVE-2026-18316	9,1	The Solace Extra plugin for WordPress	Missing Authorization	up to, and including, 1.6.0.	https://plugins.trac.wordpress.org/browser/solace-extra/tags/1.6.0/admin/class-solace-extra-admin.php#L289 https://plugins.trac.wordpress.org/browser/solace-extra/tags/1.6.0/admin/import.php#L2382 https://plugins.trac.wordpress.org/browser/solace-extra/tags/1.6.0/includes/class-solace-extra.php#L336 https://plugins.trac.wordpress.org/changeset?reponame=&old=3627961%40solace-extra&new=3627961%40solace-extra https://www.wordfence.com/threat-intel/vulnerabilities/id/4e427c4e-3e27-49e3-ba64-6241b430d5d8?source=cve	none	yes	partial
CVE-2026-19714	9,1	The Simple JWT Login WordPress plugin	Improper Authentication	before 3.6.8	https://wpscan.com/vulnerability/dc6e54eb-d856-484b-88c1-b3e04a37669d/	poc	yes	total
CVE-2026-19725	9,1	The WPvivid — Backup, Migration & Staging WordPress plugin	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	before 0.9.131	https://wpscan.com/vulnerability/999889f4-f8be-4b44-b665-1a94df8d050d/	poc	yes	total
CVE-2026-51346	9,1	StudIP	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	before 6.0.3 and 5.4.x; before 5.4.12	https://gitlab.studip.de/studip/studip/-/releases/v6.0.3 https://simon.hilchenba.ch/blog/studip-sql-injection/	poc	yes	total
CVE-2026-73041	9,0	SiYuan versions	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	versions before v3.7.4	https://github.com/siyuan-note/siyuan/security/advisories/GHSA-fqpw-c3pj-w8g9 https://www.vulncheck.com/advisories/siyuan-before-remote-code-execution-via-pdf-annotations	poc	no	total
CVE-2026-14279	8,8	The Wholesale Market plugin for WordPress	Improper Privilege Management	up to, and including, 2.2.2	https://plugins.trac.wordpress.org/browser/wholesale-market/tags/2.2.2/addons/wholesale-request/include/class-wholesale-user-register-addon.php#L141 https://plugins.trac.wordpress.org/browser/wholesale-market/tags/2.2.2/addons/wholesale-request/include/class-wholesale-user-register-addon.php#L153 https://plugins.trac.wordpress.org/browser/wholesale-market/tags/2.2.2/addons/wholesale-request/include/class-wholesale-user-register-addon.php#L276 https://plugins.trac.wordpress.org/browser/wholesale-market/tags/2.2.2/addons/wholesale-request/include/class-wholesale-user-register-addon.php#L30 https://www.wordfence.com/threat-intel/vulnerabilities/id/abd59d7a-e7f6-440d-9c2a-00266c0dcbff?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-2026-15001	8,8	The bLoyal: Loyalty & Promotions by bLoyal plugin for WordPress	Improper Privilege Management	up to, and including, 3.1.611.78.	https://plugins.trac.wordpress.org/browser/bloyal/tags/3.1.611.78/app/controller/class-bloyalcontroller.php#L2429 https://plugins.trac.wordpress.org/browser/bloyal/tags/3.1.611.78/app/controller/class-bloyalcontroller.php#L2470 https://plugins.trac.wordpress.org/browser/bloyal/tags/3.1.611.78/app/controller/class-bloyalcontroller.php#L2512 https://plugins.trac.wordpress.org/browser/bloyal/tags/3.1.611.78/app/controller/class-bloyalcontroller.php#L421 https://plugins.trac.wordpress.org/browser/bloyal/tags/3.1.611.78/app/controller/class-bloyalcontroller.php#L494 https://plugins.trac.wordpress.org/browser/bloyal/tags/3.1.611.78/app/controller/class-bloyalcontroller.php#L806	none	no	total
CVE-2026-15312	8,8	The Propovoice: All-in-One Client Management System plugin for WordPress	Improper Privilege Management	up to, and including, 1.7.8.	https://plugins.trac.wordpress.org/browser/propovoice/trunk/includes/Api/Type/Team.php#L169 https://plugins.trac.wordpress.org/browser/propovoice/trunk/includes/Api/Type/Team.php#L219 https://plugins.trac.wordpress.org/browser/propovoice/trunk/includes/Api/Type/Team.php#L38 https://plugins.trac.wordpress.org/browser/propovoice/trunk/includes/Api/Type/Team.php#L423 https://www.wordfence.com/threat-intel/vulnerabilities/id/6a39e4d4-890d-46f9-8bb9-0fc858e6f1e2?source=cve			
CVE-2026-15965	8,8	The MaxUpload – Big File Uploads – Increase Maximum File Upload Size plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 1.4.0	https://plugins.trac.wordpress.org/browser/maxupload-upload-larger-files-easily/tags/1.4.0/includes/uploader.php#L121 https://plugins.trac.wordpress.org/browser/maxupload-upload-larger-files-easily/tags/1.4.0/includes/uploader.php#L174 https://plugins.trac.wordpress.org/browser/maxupload-upload-larger-files-easily/tags/1.4.0/includes/uploader.php#L19 https://plugins.trac.wordpress.org/browser/maxupload-upload-larger-files-easily/tags/1.4.0/includes/uploader.php#L201 https://plugins.trac.wordpress.org/browser/maxupload-upload-larger-files-easily/tags/1.4.0/maxupload-wp.php#L88 https://www.wordfence.com/threat-intel/vulnerabilities/id/70d90c0c-e3c6-4db9-b16d-1442e7e1dc3b?source=cve	none	no	total
CVE-2026-16099	8,8	The Podlove Podcast Publisher plugin for WordPress	Deserialization of Untrusted Data	up to, and including, 4.5.3.	https://plugins.trac.wordpress.org/browser/podlove-podcasting-plugin-for-wordpress/tags/4.5.3/lib/image_cache/generation_guard.php#L19 https://plugins.trac.wordpress.org/browser/podlove-podcasting-plugin-for-wordpress/tags/4.5.3/lib/image_cache/generation_guard.php#L57 https://plugins.trac.wordpress.org/browser/podlove-podcasting-plugin-for-wordpress/tags/4.5.3/lib/model/base.php#L552 https://plugins.trac.wordpress.org/browser/podlove-podcasting-plugin-for-wordpress/tags/4.5.3/lib/modules/shownotes/rest_api.php#L538 https://plugins.trac.wordpress.org/browser/podlove-podcasting-plugin-for-wordpress/tags/4.5.3/lib/modules/shownotes/rest_api.php#L585 https://plugins.trac.wordpress.org/browser/podlove-podcasting-plugin-for-wordpress/tags/4.5.3/lib/modules/shownotes/rest_api.php#L630	none	no	total
CVE-2026-17123	8,8	The Royal Elementor Addons plugin for WordPress	Server-Side Request Forgery (SSRF)	up to, and including, 1.7.1064	https://plugins.trac.wordpress.org/browser/royal-elementor-addons/tags/1.7.1061/classes/modules/forms/wpr-send-webhook.php#L20 https://plugins.trac.wordpress.org/browser/royal-elementor-addons/tags/1.7.1061/classes/modules/forms/wpr-send-webhook.php#L56 https://plugins.trac.wordpress.org/browser/royal-elementor-addons/tags/1.7.1061/modules/form-builder/widgets/wpr-form-builder.php#L3788 https://plugins.trac.wordpress.org/browser/royal-elementor-addons/tags/1.7.1064/classes/modules/forms/wpr-send-webhook.php#L20 https://plugins.trac.wordpress.org/browser/royal-elementor-addons/tags/1.7.1064/classes/modules/forms/wpr-send-webhook.php#L56 https://plugins.trac.wordpress.org/browser/royal-elementor-addons/tags/1.7.1064/modules/form-builder/widgets/wpr-form-builder.php#L3788	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-2026-18438	8,8	The Templately – Elementor & Gutenberg Template Library	Unrestricted Upload of File with Dangerous Type	up to, and including, 3.7.1	https://plugins.trac.wordpress.org/browser/templately/tags/3.6.5/includes/API/API.php#L128 https://plugins.trac.wordpress.org/browser/templately/tags/3.6.5/includes/API/Import.php#L78 https://plugins.trac.wordpress.org/browser/templately/tags/3.6.5/includes/API/MyClouds.php#L103 https://plugins.trac.wordpress.org/browser/templately/tags/3.6.5/includes/Core/Importer/WPImport.php#L1200 https://plugins.trac.wordpress.org/browser/templately/tags/3.6.5/includes/Core/Importer/WPImport.php#L1391 https://plugins.trac.wordpress.org/browser/templately/tags/3.6.5/includes/Core/Importer/WPImport.php#L1423	none	no	total
CVE-2026-62982	8,8	Glances	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	>= 4.5.2, < 4.5.6	https://github.com/nicolargo/glances/commit/ea4cf2f54f0d961e24aa0b24fff9584bab39db93 https://github.com/nicolargo/glances/releases/tag/v4.5.6 https://github.com/nicolargo/glances/security/advisories/GHSA-73wf-9vmv-5pv9	poc	no	total
CVE-2026-70495	8,8	search-v2-operator	Improper Privilege Management		https://access.redhat.com/security/cve/CVE-2026-70495 https://bugzilla.redhat.com/show_bug.cgi?id=2511031			
CVE-2026-72462	8,8	unix socket mediation when peer_path		bc6e5f6933b8e7b74858ac830d5b9b4ca10a099a prior to d8ea44f6090c087fe255d9512fb808574b4d88e8; bc6e5f6933b8e7b74858ac830d5b9b4ca10a099a prior to d680472db98823d90fc91362910901e468269318; bc6e5f6933b8e7b74858ac830d5b9b4ca10a099a prior to b1aea2c1960771a276d7e68c7424168eccd0c3da; 6.17	https://git.kernel.org/stable/c/b1aea2c1960771a276d7e68c7424168eccd0c3da https://git.kernel.org/stable/c/d680472db98823d90fc91362910901e468269318 https://git.kernel.org/stable/c/d8ea44f6090c087fe255d9512fb808574b4d88e8			
CVE-2026-74490	8,8	poll trace queue dumps TIPC socket tracepoints dump queue state		b4b9771bcbbd5839b0f77aba55e2f85989ed6779 prior to d7940bb6a8e7ab28f972c2875cb05783216312dc; b4b9771bcbbd5839b0f77aba55e2f85989ed6779 prior to 5e82beba4bc1f91d0e64c9c43f2b2fa9cd1c2a7d; b4b9771bcbbd5839b0f77aba55e2f85989ed6779 prior to bed792737b5f1ba773054dbe984502958bdfe6ce; b4b9771bcbbd5839b0f77aba55e2f85989ed6779 prior to ac2f787980fdf4364cd5651a4c8128e59b8de3aa; b4b9771bcbbd5839b0f77aba55e2f85989ed6779 prior to b4f1719dfea023220e0e6bd892b087d76b2a6a49; 5.0	https://git.kernel.org/stable/c/5e82beba4bc1f91d0e64c9c43f2b2fa9cd1c2a7d https://git.kernel.org/stable/c/ac2f787980fdf4364cd5651a4c8128e59b8de3aa https://git.kernel.org/stable/c/b4f1719dfea023220e0e6bd892b087d76b2a6a49 https://git.kernel.org/stable/c/bed792737b5f1ba773054dbe984502958bdfe6ce https://git.kernel.org/stable/c/d7940bb6a8e7ab28f972c2875cb05783216312dc			
CVE-2026-74522	8,8	__close_file_table_ids() A ksmbd_file		8510a043d334ecdf83d4604782f288db6bf21d60 prior to 67aaec2a1fdce3e1dde46c45b5d1ef8cf22f65cd; 8510a043d334ecdf83d4604782f288db6bf21d60 prior to 0c3918c2cee62ec6c9de8d5c73ebfe6f833961ac; 8510a043d334ecdf83d4604782f288db6bf21d60 prior to 9be4a66f019ea90bd9deca70511f4f9ffebf5c6f; 8510a043d334ecdf83d4604782f288db6bf21d60 prior to cffbdc86393b0235383a20c8c59bc32f16036459; 8510a043d334ecdf83d4604782f288db6bf21d60 prior to e7188199eff46a636f3436356f0aae039be6dd66; df30cbfd3d8a70e61ce59f63ce5ed2261799ac10; aaf1d5ebb358f546414965b39da90107a7ca7ce5; 5.15.38 prior to 5.16; 5.17.6 prior to 5.18; 5.18	https://git.kernel.org/stable/c/0c3918c2cee62ec6c9de8d5c73ebfe6f833961ac https://git.kernel.org/stable/c/67aaec2a1fdce3e1dde46c45b5d1ef8cf22f65cd https://git.kernel.org/stable/c/9be4a66f019ea90bd9deca70511f4f9ffebf5c6f https://git.kernel.org/stable/c/cffbdc86393b0235383a20c8c59bc32f16036459 https://git.kernel.org/stable/c/e7188199eff46a636f3436356f0aae039be6dd66			
CVE-2026-74530	8,8	hci_connect_big_sync() callback There		024421cf39923927ab2b5fe895d1d922b9abe67f prior to 2d91e6244b69d752503b2d44020d8b0e323dbd38; 024421cf39923927ab2b5fe895d1d922b9abe67f prior to 56e78b670356caab0b607e8aad4cf819a1909d07; 620810ac1f7f1133a9ac403e132b3ad6995ddf39; ee0586ad64a805eaf1a9a10100e908627a561e34; 6.12.28 prior to 6.13; 6.14.6 prior to 6.15; 6.15	https://git.kernel.org/stable/c/2d91e6244b69d752503b2d44020d8b0e323dbd38 https://git.kernel.org/stable/c/56e78b670356caab0b607e8aad4cf819a1909d07			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-74535	8,8	iso_sock_timeout iso_sock_timeout() takes lock_sock, so sync disabling the timer while holding that lock		a58d0f5dac322e16cc75334d000666512341bde5 prior to 16d89a63e08280abeef7218970a3bbd7ca62b021; dc26097bdb864a0d5955b9a25e43376ffc1af99b prior to 82e982f54f962f72646868ddbb2c3bd9ea178568; dc26097bdb864a0d5955b9a25e43376ffc1af99b prior to 3c3d5f85db80145636bb991a6005e2760012b985; dc26097bdb864a0d5955b9a25e43376ffc1af99b prior to 200fa1629c57a3ca2b03d3ca63fd3a9bfd910c43; f53e7489273dc2bb307bf50f319b3762d45534f0; 6.12.2 prior to 6.12.103; 6.11.11 prior to 6.12; 6.13	https://git.kernel.org/stable/c/16d89a63e08280abeef7218970a3bbd7ca62b021 https://git.kernel.org/stable/c/200fa1629c57a3ca2b03d3ca63fd3a9bfd910c43 https://git.kernel.org/stable/c/3c3d5f85db80145636bb991a6005e2760012b985 https://git.kernel.org/stable/c/82e982f54f962f72646868ddbb2c3bd9ea178568			
CVE-2026-74538	8,8	iso_connect_ind Accessing iso_pi(sk)->conn requires lock_sock, which		168d9bf9c7f01df71e6404cfff66d9c2a8e968fb prior to e8e9cff6d80eeec28dec4cf7cc18662986945391; 168d9bf9c7f01df71e6404cfff66d9c2a8e968fb prior to 9bee7e476534f27e830658dad962d85da9edf6bf; 168d9bf9c7f01df71e6404cfff66d9c2a8e968fb prior to 4311fd6f429065a8ba208660360a895627a00cf3; 489efc9ae36f164423f5fa7ace772a7ab8131cd8; 6.8.9 prior to 6.9; 6.9	https://git.kernel.org/stable/c/4311fd6f429065a8ba208660360a895627a00cf3 https://git.kernel.org/stable/c/9bee7e476534f27e830658dad962d85da9edf6bf https://git.kernel.org/stable/c/e8e9cff6d80eeec28dec4cf7cc18662986945391			
CVE-2026-74997	8,8	In Roundcube Webmail	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	before 1.6.18 and 1.7.x; before 1.7.3	https://github.com/roundcube/roundcubemail/commit/14044f843cfacbe78b042f659e379d6b4497aa7c https://github.com/roundcube/roundcubemail/commit/495d211638f222336b20f4744545c53712426c2a https://github.com/roundcube/roundcubemail/commit/b8f90e28a46d42e79a69568cba897f8f4223d9cd https://github.com/roundcube/roundcubemail/releases/tag/1.6.18 https://github.com/roundcube/roundcubemail/releases/tag/1.7.3 https://roundcube.net/news/2026/08/09/security-updates-1.6.18-and-1.7.3	none	no	total
CVE-2026-9771	8,8	drivers/flash/flash_util	Untrusted Pointer Dereference; Missing Authorization	4.0.0 prior to 4.4.2	https://github.com/zephyrproject-rtos/zephyr/commit/1b1ecdc438092cdd469319a0d51cba6cf82e06f4 https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-68cj-3hg4-5vpm	none	no	total
CVE-2026-57485	8,5	Stirling-PDF	Exposure of Sensitive Information to an Unauthorized Actor; Insufficiently Protected Credentials	Prior to 2.9.0	https://github.com/Stirling-Tools/Stirling-PDF/commit/de9625942bbc329fdefcfde161476a633a3b3213 https://github.com/Stirling-Tools/Stirling-PDF/pull/6047 https://github.com/Stirling-Tools/Stirling-PDF/releases/tag/v2.9.0 https://github.com/Stirling-Tools/Stirling-PDF/security/advisories/GHSA-3xxh-mm3g-c9w5			
CVE-2026-72310	8,1	passthrough ioctl bounds check smb2_ioctl_query_info() validates the PASSTHRU_FSCTL response payload		2b1116bbe898aefdf584838448c6869f69851e0f prior to 175357ee0c596cb82054650dfa32fda51ad35aaa; 2b1116bbe898aefdf584838448c6869f69851e0f prior to dbd126539c098dba3159ce7d34b10b2daddcbd0f; 2b1116bbe898aefdf584838448c6869f69851e0f prior to 63feb687e89a3a52a31e6e01764117cc500f1974; 2b1116bbe898aefdf584838448c6869f69851e0f prior to 160045fc943f6c46b227644261252c8a22b8a87a; 2b1116bbe898aefdf584838448c6869f69851e0f prior to b30771b69eafae750afb7385fbcc3d77ed3f3670; 2b1116bbe898aefdf584838448c6869f69851e0f prior to 1627e7d5c9b09721a141d07cedb178882f1ded67; 2b1116bbe898aefdf584838448c6869f69851e0f prior to 1a638c55f2db6cb2296e5e3138015dd8fd9d4aa9; 2b1116bbe898aefdf584838448c6869f69851e0f prior to a4f27ad055392fa164f5649e89a3637b033c5fcc; 2005c32ec99ee2490e8131b3953f3f212009ffea; 5.4.69 prior to 5.5; 5.5	https://git.kernel.org/stable/c/160045fc943f6c46b227644261252c8a22b8a87a https://git.kernel.org/stable/c/1627e7d5c9b09721a141d07cedb178882f1ded67 https://git.kernel.org/stable/c/175357ee0c596cb82054650dfa32fda51ad35aaa https://git.kernel.org/stable/c/1a638c55f2db6cb2296e5e3138015dd8fd9d4aa9 https://git.kernel.org/stable/c/63feb687e89a3a52a31e6e01764117cc500f1974 https://git.kernel.org/stable/c/a4f27ad055392fa164f5649e89a3637b033c5fcc			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-74528	8,0	hci_past_sync() callback Avoids giv- ing freed pointers to hci_conn_valid(), which kmalloc		d3413703d5f8b7d1e6f514f9440ed5da1bc30796 prior to e6792adef614b389141b142e30ee549e4a47dd7d; d3413703d5f8b7d1e6f514f9440ed5da1bc30796 prior to abf9753edf3f88282c44a605f3945d8d4f8dd86c; 6.19	https://git.kernel.org/stable/c/abf9753edf3f88282c44a605f3945d8d4f8dd86c https://git.kernel.org/stable/c/e6792adef614b389141b142e30ee549e4a47dd7d			
CVE-2026-74539	8,0	iso_sock_getname Accessing iso_pi(sk)- >conn requires lock_sock, which		2df108c227b266a9ec9e3fda3828d2ac9662aa33 prior to 72d5bb1d77d7c3330146dc0cfd43f704c64b9594; 2df108c227b266a9ec9e3fda3828d2ac9662aa33 prior to 202670e6602e068558c1fca2df40719ee91a2906; 2df108c227b266a9ec9e3fda3828d2ac9662aa33 prior to 89cf154d7c18e6e94a3da83051f3cf2bac317ae2; 6.16	https://git.kernel.org/stable/c/202670e6602e068558c1fca2df40719ee91a2906 https://git.kernel.org/stable/c/72d5bb1d77d7c3330146dc0cfd43f704c64b9594 https://git.kernel.org/stable/c/89cf154d7c18e6e94a3da83051f3cf2bac317ae2			
CVE-2026-15218	7,9	the maas-api and maas-controller Ser- viceAccounts within Red Hat OpenShift AI	Incorrect Privilege Assignment		https://access.redhat.com/security/cve/CVE-2026-15218 https://bugzilla.redhat.com/show_bug.cgi?id=2498426	none	no	total
CVE-2026-72114	7,8	bcm_rx_setup() for RTR replies bcm_tx_setup() vali- dates cf->len against the		ffd980f976e7fd666c2e61bf8ab35107efd11828 prior to 7d966cdee006911d3957e1a4e72cb93c39cd8c1e; ffd980f976e7fd666c2e61bf8ab35107efd11828 prior to 1b475c0c72f44622a320a4386ce9e76f85e69bc7; ffd980f976e7fd666c2e61bf8ab35107efd11828 prior to deb6a697cce3f021e731df543597f37a5e54caab; ffd980f976e7fd666c2e61bf8ab35107efd11828 prior to 59bfddea64159594feb62ef11b7d7a33c8ee3783; ffd980f976e7fd666c2e61bf8ab35107efd11828 prior to 62ec41f364648be79d54d94d0d240ee326948afd; 2.6.25	https://git.kernel.org/stable/c/1b475c0c72f44622a320a4386ce9e76f85e69bc7 https://git.kernel.org/stable/c/59bfddea64159594feb62ef11b7d7a33c8ee3783 https://git.kernel.org/stable/c/62ec41f364648be79d54d94d0d240ee326948afd https://git.kernel.org/stable/c/7d966cdee006911d3957e1a4e72cb93c39cd8c1e https://git.kernel.org/stable/c/deb6a697cce3f021e731df543597f37a5e54caab			
CVE-2026-72165	7,8	'nand_select_target()' 'cs' here must be in range [0:nanddev_ntargets[		32813e288414fecce18f37f8f0d0414a64b45c56 prior to 483a8a8581ee1274ec70e2561492096d4a7305e6; 32813e288414fecce18f37f8f0d0414a64b45c56 prior to c2a131fb6882c98aada739479cc96df8748d0c24; 32813e288414fecce18f37f8f0d0414a64b45c56 prior to e6df4fea1dc86c058e1918136c9b9d8e80c4be1b; 32813e288414fecce18f37f8f0d0414a64b45c56 prior to 3da4eb15c7b421c2d97c402bb7bd607c44822995; 32813e288414fecce18f37f8f0d0414a64b45c56 prior to fbc7c8a1167b2eb56b2fd8598c29a3d5e9f8676e; 32813e288414fecce18f37f8f0d0414a64b45c56 prior to 4bbfcf9c7e46cae58257150bf834853559382e28; 32813e288414fecce18f37f8f0d0414a64b45c56 prior to 8f575fc17360827ca1d1940a84f3c7ee40407a10; 32813e288414fecce18f37f8f0d0414a64b45c56 prior to 8507c2cc9e4fa402401819f44d1e8a5ef4d11d8b; 5.2	https://git.kernel.org/stable/c/3da4eb15c7b421c2d97c402bb7bd607c44822995 https://git.kernel.org/stable/c/483a8a8581ee1274ec70e2561492096d4a7305e6 https://git.kernel.org/stable/c/4bbfcf9c7e46cae58257150bf834853559382e28 https://git.kernel.org/stable/c/8507c2cc9e4fa402401819f44d1e8a5ef4d11d8b https://git.kernel.org/stable/c/8f575fc17360827ca1d1940a84f3c7ee40407a10 https://git.kernel.org/stable/c/c2a131fb6882c98aada739479cc96df8748d0c24			
CVE-2026-72170	7,8	cacheless mode to fix WARN_ON v9fs_dec_count() un- conditionally calls drop_nlink() on regu- lar files, even when the inode's nlink		ac89b2ef9b55924bcf922251f043ba73a32d05bb prior to a5a682b016ef5b5384e28f6d652d47a8f8e73d37; ac89b2ef9b55924bcf922251f043ba73a32d05bb prior to de79c3f3643841b8659a71958df7cf2a66bfd409; ac89b2ef9b55924bcf922251f043ba73a32d05bb prior to 8d610017c992de705b304d3d727a6e3a86af6149; ac89b2ef9b55924bcf922251f043ba73a32d05bb prior to 8faccac11e1369adddf5d80f4a45af93f13b2e1a; ac89b2ef9b55924bcf922251f043ba73a32d05bb prior to 574aa0b4799470ac814479f1138d19efe6262255; 4.17	https://git.kernel.org/stable/c/574aa0b4799470ac814479f1138d19efe6262255 https://git.kernel.org/stable/c/8d610017c992de705b304d3d727a6e3a86af6149 https://git.kernel.org/stable/c/8faccac11e1369adddf5d80f4a45af93f13b2e1a https://git.kernel.org/stable/c/a5a682b016ef5b5384e28f6d652d47a8f8e73d37 https://git.kernel.org/stable/c/de79c3f3643841b8659a71958df7cf2a66bfd409			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-72195	7,8	UpdateResi-dentValue against data_off In do_ac-tion()'s UpdateResi-dentValue case (fslog		up to 4	https://git.kernel.org/stable/c/50b5e83384e7fed3d11d18b79ff350e9d6d89861 https://git.kernel.org/stable/c/53c12f178f584dc5f836ffe2782138a6e9348ed9 https://git.kernel.org/stable/c/546518468e6c9ea469669eef78f8cc380ad6e2ca https://git.kernel.org/stable/c/97758fd9756b5f09e9ddc6a5f6a569041acc8421 https://git.kernel.org/stable/c/a89c66674283a0293c0f266dc57087a6114371a3 https://git.kernel.org/stable/c/ab8761676d638c5be170aaf91b7ffdd451236616			
CVE-2026-72368	7,8	nomem_d_alloc error path When start_cre-ating() fails and re-turns -ENOMEM, it		7ab96df840e60eb933abfe65fc5fe44e72f16dc0 prior to 26757dac15175f2a42e3537f1ba86e62456d48f1; 7ab96df840e60eb933abfe65fc5fe44e72f16dc0 prior to 8c256fba2b46020004201c500b2a1fbc707a33ef; 6.19	https://git.kernel.org/stable/c/26757dac15175f2a42e3537f1ba86e62456d48f1 https://git.kernel.org/stable/c/8c256fba2b46020004201c500b2a1fbc707a33ef			
CVE-2026-72369	7,8	bitmap block count calculation minix_check_superb-lock() uses minix_blocks_neede d() to verify that the on-disk imap and zmap block counts		2bb588cede1c1969e49c0a2822c8cb8b346b7682 prior to a11ebaab50d27d6c4c78506f84ff36452e0b901d; f57ccd4657c7f082dc47e5b9e18a883bb5f9118f prior to 959c95340a9e19cd333b4c18935fdeecbb2f319d; 31fefc18096cdc5549cfa54964d90e0b3229aedc prior to abe3536a4bedcc43de80b6d4d7e3d57e9ba382a5; 8c97a6ddc95690a938ded44b4e3202f03f15078c prior to 8a29e60e2176b02e04f8737c8b32b696230eb0c5; 8c97a6ddc95690a938ded44b4e3202f03f15078c prior to fb3e566cafc38fe3ba35e6843a2d529a3748870c; a051ecf5c5b0387840dc210413ed3bc7fbdaa69c; d791c544efd6b9c944b43cf7f502e5bcb02fb941; 66c7c239c65341f99ae388d4d53dc9df2bcb9925; 1efc128ee4adbc23e082715425ff895449d233bc; 6.6.128 prior to 6.6.145; 6.12.75 prior to 6.12.97; 6.18.16 prior to 6.18.40; 5.10.252 prior to 5.11; 5.15.202 prior to 5.16; 6.1.165 prior to 6.2; 6.19.6 prior to 6.20; 7.0	https://git.kernel.org/stable/c/8a29e60e2176b02e04f8737c8b32b696230eb0c5 https://git.kernel.org/stable/c/959c95340a9e19cd333b4c18935fdeecbb2f319d https://git.kernel.org/stable/c/a11ebaab50d27d6c4c78506f84ff36452e0b901d https://git.kernel.org/stable/c/abe3536a4bedcc43de80b6d4d7e3d57e9ba382a5 https://git.kernel.org/stable/c/fb3e566cafc38fe3ba35e6843a2d529a3748870c			
CVE-2026-72383	7,8	sctp_free_addr_wq() sctp_free_addr_wq() previously removed addr_wq_timer using timer_delete() while holding addr_wq_lock		4db67e808640e3934d82ce61ee8e2e89fd877ba8 prior to a8323fb2ab6cd6978f359daeed6688e0cadf32ba; 4db67e808640e3934d82ce61ee8e2e89fd877ba8 prior to c3e5cac47519d77ad36b9c03a1df1536aaa0c4a1; 4db67e808640e3934d82ce61ee8e2e89fd877ba8 prior to 976c19de0f22a857ba0112f39635f8fd7a257568; 3.7	https://git.kernel.org/stable/c/976c19de0f22a857ba0112f39635f8fd7a257568 https://git.kernel.org/stable/c/a8323fb2ab6cd6978f359daeed6688e0cadf32ba https://git.kernel.org/stable/c/c3e5cac47519d77ad36b9c03a1df1536aaa0c4a1			
CVE-2026-72404	7,8	cleanup_bearer() due to premature dst_cache_destroy() TIPC UDP media bearer teardown calls dst_cache_destroy() on its replicast caches		e9c1a793210f29f32ee4cf048e04d7d9bb3221cc prior to 1c8393eefa3cadf4ca0b61119ad1321aa32d3c8c; e9c1a793210f29f32ee4cf048e04d7d9bb3221cc prior to 7116764ca53ff529335d7ab7c364a69f094b23a5; 5.3	https://git.kernel.org/stable/c/1c8393eefa3cadf4ca0b61119ad1321aa32d3c8c https://git.kernel.org/stable/c/7116764ca53ff529335d7ab7c364a69f094b23a5			
CVE-2026-72454	7,8	i3c_hci_addr_to_dev( ) i3c_hci_addr_to_dev( ) walks bus->devs		9ad9a52cce2828d932ae9495181e3d6414f72c07 prior to 8f851cab401c28287d536b1347d76f6e219c0db6; 9ad9a52cce2828d932ae9495181e3d6414f72c07 prior to 650716f23eac488c6696babdc7805f6a6b7427ad; 5.11	https://git.kernel.org/stable/c/650716f23eac488c6696babdc7805f6a6b7427ad https://git.kernel.org/stable/c/8f851cab401c28287d536b1347d76f6e219c0db6			
CVE-2026-74257	7,8	udp_bpf_recvmsg() syzbot reported use-after-free of struct sk_msg in sk_msg_recvmsg()		9f2470fbc4cb4583c080bb729a998933ba61aca4 prior to 81567d2b3f4dc4fc32f8b61433738bce2cafd4a1; 9f2470fbc4cb4583c080bb729a998933ba61aca4 prior to 39d44ed6904bfa9a1c6d0538672dd50c7b85520e; 9f2470fbc4cb4583c080bb729a998933ba61aca4 prior to c010995b29c8939c6aa69e3cb26f8dbee163d156; 5.14	https://git.kernel.org/stable/c/39d44ed6904bfa9a1c6d0538672dd50c7b85520e https://git.kernel.org/stable/c/81567d2b3f4dc4fc32f8b61433738bce2cafd4a1 https://git.kernel.org/stable/c/c010995b29c8939c6aa69e3cb26f8dbee163d156			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-74302	7,8	hci_unregister_dev() hci_unregister_dev() does not disable cmd_timer and ncmd_timer		0d151a103775dd9645c78c97f77d6e2a5298d913 prior to 48c7ad6afcc58c2cda11fed39791708103b6a644; 0d151a103775dd9645c78c97f77d6e2a5298d913 prior to a0fd1086a57b982f8c24ae4ab165c2af39fe1735; 0d151a103775dd9645c78c97f77d6e2a5298d913 prior to 672d52d9412252e61b8de8d773ccdf5a277cf540; 0d151a103775dd9645c78c97f77d6e2a5298d913 prior to 5edcc018fa6e80b2c478454a4a8229c23d67c181; 48542881997e17b49dc16b93fe910e0cfcf7a9f9; 9cfc84b1d464cc024286f42a090718f9067b80ed; ddeda6ca5f218b668b560d90fc31ae469adbfd92; d2ce562a5aff1dcd0c50d9808ea825ef90da909f; 96600c2e5ee8213dbab5df1617293d8e847bb4fa; d6cbce18370641a21dd889e8613d8153df15eb39; 3f939bd73fed12dddc2a32a76116c19ca47c7678; 4.19.319 prior to 4.20; 5.4.281 prior to 5.5; 5.10.223 prior to 5.11; 5.15.164 prior to 5.16; 6.1.101 prior to 6.2; 6.6.42 prior to 6.7; 6.9.11 prior to 6.10; 6.10	https://git.kernel.org/stable/c/48c7ad6afcc58c2cda11fed39791708103b6a644 https://git.kernel.org/stable/c/5edcc018fa6e80b2c478454a4a8229c23d67c181 https://git.kernel.org/stable/c/672d52d9412252e61b8de8d773ccdf5a277cf540 https://git.kernel.org/stable/c/a0fd1086a57b982f8c24ae4ab165c2af39fe1735			
CVE-2026-74306	7,8	qat_vf_resume_write() qat_vf_resume_write() checks filp->f_pos		bb208810b1abf1c84870cfbe1cc9cf1a1d35c607 prior to 6465af0004dc1b067129a26ef44f19cdf13bbce6; bb208810b1abf1c84870cfbe1cc9cf1a1d35c607 prior to d416dcefdbac90d96b22485fd93f28229ad9984b; bb208810b1abf1c84870cfbe1cc9cf1a1d35c607 prior to b6fd7a40a66485c8aa8156d8fcf50b95cb8ba281; bb208810b1abf1c84870cfbe1cc9cf1a1d35c607 prior to 4ec5e932e636896e97e4c6a8205b0ac76d52421a; 6.10	https://git.kernel.org/stable/c/4ec5e932e636896e97e4c6a8205b0ac76d52421a https://git.kernel.org/stable/c/6465af0004dc1b067129a26ef44f19cdf13bbce6 https://git.kernel.org/stable/c/b6fd7a40a66485c8aa8156d8fcf50b95cb8ba281 https://git.kernel.org/stable/c/d416dcefdbac90d96b22485fd93f28229ad9984b			
CVE-2026-74354	7,8	zap_pages() zap_vma_range() requires the owning mm's mmap_lock to be held		317460317a02a1af512697e6e964298dedd8a163 prior to 36b1d997866f6083d33934983aa2ce0a184ed642; 317460317a02a1af512697e6e964298dedd8a163 prior to 80b89d0226a05e8b67969de99c31b51fcd54f76a; 6.9	https://git.kernel.org/stable/c/36b1d997866f6083d33934983aa2ce0a184ed642 https://git.kernel.org/stable/c/80b89d0226a05e8b67969de99c31b51fcd54f76a			
CVE-2026-74496	7,8	fou_create() fou_create() publishes struct fou		23461551c00628c3f3fe9cf837bf53cf8f212b63 prior to a28d8903bfe76089ea4bbdbff9976965f9ef8107; 23461551c00628c3f3fe9cf837bf53cf8f212b63 prior to b14361aca6350ff7907b0e9903c7b94dc7d5d4a0; 3.18	https://git.kernel.org/stable/c/a28d8903bfe76089ea4bbdbff9976965f9ef8107 https://git.kernel.org/stable/c/b14361aca6350ff7907b0e9903c7b94dc7d5d4a0			
CVE-2026-74518	7,8	allocate_file_region_entries() allocate_file_region_entries() tops up resv->region_cache with freshly allocated file_region descriptors		d3ec7b6e09e512ba902b86bcca2c512fb06d492f prior to 62e1c2741a4d923d9854efd5927a6212aad7a187; d3ec7b6e09e512ba902b86bcca2c512fb06d492f prior to 587a0accc2b4fccc5cf7baf0fe34e50efde51f9c; d3ec7b6e09e512ba902b86bcca2c512fb06d492f prior to 126a70bf1a08ddc9d79c471ebdaa2b08cfbab8df; d3ec7b6e09e512ba902b86bcca2c512fb06d492f prior to ac1bb7fd45088d0db57a22ce7729f258ebd63cf5; d3ec7b6e09e512ba902b86bcca2c512fb06d492f prior to dd9623f58ec702a07b2d67179d6fcea79c52231a; 5.10	https://git.kernel.org/stable/c/126a70bf1a08ddc9d79c471ebdaa2b08cfbab8df https://git.kernel.org/stable/c/587a0accc2b4fccc5cf7baf0fe34e50efde51f9c https://git.kernel.org/stable/c/62e1c2741a4d923d9854efd5927a6212aad7a187 https://git.kernel.org/stable/c/ac1bb7fd45088d0db57a22ce7729f258ebd63cf5 https://git.kernel.org/stable/c/dd9623f58ec702a07b2d67179d6fcea79c52231a			
CVE-2026-74529	7,8	hci_connect_pa_sync() callback There		6d0417e4e1cf66fd917f06f0454958362714ef7d prior to c53c70ec289ee12f20c4f1b2fbfd151762c01f67; 6d0417e4e1cf66fd917f06f0454958362714ef7d prior to 44fc74069d8988f2825246f9401218e29de2c0ab; eb8b860e87b296bd1874c79a668081efd00f9754; 94bf6380e936339a700c0b3171a49baf512aa70b; 6.12.28 prior to 6.13; 6.14.6 prior to 6.15; 6.15	https://git.kernel.org/stable/c/44fc74069d8988f2825246f9401218e29de2c0ab https://git.kernel.org/stable/c/c53c70ec289ee12f20c4f1b2fbfd151762c01f67			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-15162	7,5	The Object Sync for Salesforce plugin	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	2.2.13 and earlier	https://plugins.trac.wordpress.org/browser/object-sync-for-salesforce/trunk/classes/class-object-sync-sf-rest.php#L224 https://plugins.trac.wordpress.org/browser/object-sync-for-salesforce/trunk/classes/class-object-sync-sf-salesforce-push.php#L210 https://plugins.trac.wordpress.org/browser/object-sync-for-salesforce/trunk/classes/class-object-sync-sf-wordpress.php#L328 https://plugins.trac.wordpress.org/browser/object-sync-for-salesforce/trunk/classes/class-object-sync-sf-wordpress.php#L578 https://www.wordfence.com/threat-intel/vulnerabilities/id/78f964a7-bed3-435e-94c5-750883a0c836?source=cve	none	yes	partial
CVE-2026-16611	7,5	The Product Feed PRO for WooCommerce by AdTribes WordPress plugin	Exposure of Sensitive Information to an Unauthorized Actor	before 13.5.7	https://wpscan.com/vulnerability/87fe63af-5a43-4812-88ce-568b1cc1598f/	poc	yes	partial
CVE-2026-17087	7,5	The WP Travel Engine – Tour Booking Plugin – Tour Operator Software plugin for WordPress	Missing Authorization	up to, and including, 6.8.4.	https://plugins.trac.wordpress.org/browser/wp-travel-engine/tags/6.7.12/includes/classes/Abstracts/AjaxController.php#L52 https://plugins.trac.wordpress.org/browser/wp-travel-engine/tags/6.7.12/includes/classes/Builders/FormFields/BillingFormFields.php#L87 https://plugins.trac.wordpress.org/browser/wp-travel-engine/tags/6.7.12/includes/classes/Core/Controllers/Ajax/AddToCart.php#L232 https://plugins.trac.wordpress.org/browser/wp-travel-engine/tags/6.7.12/includes/classes/Core/Controllers/Ajax/AddToCart.php#L31 https://plugins.trac.wordpress.org/browser/wp-travel-engine/tags/6.7.12/includes/classes/Legacy/Cart.php#L373 https://plugins.trac.wordpress.org/browser/wp-travel-engine/tags/6.8.3/includes/classes/Abstracts/AjaxController.php#L52	none	yes	partial
CVE-2026-19717	7,5	The CatFolders Document Gallery & PDF Library WordPress plugin	Exposure of Sensitive Information to an Unauthorized Actor	before 2.0.7	https://wpscan.com/vulnerability/79a4bae6-96e2-44b4-a56b-42198f8b3d32/	poc	yes	partial
CVE-2026-19728	7,5	The Extra Product Options Builder for WooCommerce WordPress plugin	Missing Authorization	before 1.2.176	https://wpscan.com/vulnerability/fd10aaab-d358-4d2f-aafa-dbfba09b7fff/	poc	yes	partial
CVE-2026-72378	7,5	afs_extract_vl_addrs() The error codes on these paths		0a5143f2f89cc88d8a3eada8e8ccd86c1e988257 prior to 7ce6737a975ea3e0dc2e5946628d233779ca0caf; 0a5143f2f89cc88d8a3eada8e8ccd86c1e988257 prior to 4e0b047848a855f2c933a6439f76a01743ba5620; 0a5143f2f89cc88d8a3eada8e8ccd86c1e988257 prior to f70fbf2b974b63a7042705c2b0464cb8c97e9f34; 0a5143f2f89cc88d8a3eada8e8ccd86c1e988257 prior to 9ad9016e3333c3c1f9284a253ff0658369e07aac; 0a5143f2f89cc88d8a3eada8e8ccd86c1e988257 prior to cb33dd2968588c78fad78dec19f61cabe5785494; 0a5143f2f89cc88d8a3eada8e8ccd86c1e988257 prior to 8530206911fd66ad739ca5ce95f1d069f3d42204; 0a5143f2f89cc88d8a3eada8e8ccd86c1e988257 prior to bdcd80ff12939d172043fac5eb822b92366a1bab; 0a5143f2f89cc88d8a3eada8e8ccd86c1e988257 prior to 4897cb71d4ab1f7e1a214adb1e4b80176702368d; 4.20	https://git.kernel.org/stable/c/4897cb71d4ab1f7e1a214adb1e4b80176702368d https://git.kernel.org/stable/c/4e0b047848a855f2c933a6439f76a01743ba5620 https://git.kernel.org/stable/c/7ce6737a975ea3e0dc2e5946628d233779ca0caf https://git.kernel.org/stable/c/8530206911fd66ad739ca5ce95f1d069f3d42204 https://git.kernel.org/stable/c/9ad9016e3333c3c1f9284a253ff0658369e07aac https://git.kernel.org/stable/c/bdcd80ff12939d172043fac5eb822b92366a1bab			
CVE-2026-73634	7,5	Apache Struts	Uncontrolled Resource Consumption	from 6.0.0 through 6.10.0; from 7.0.0 through 7.2.1.	https://cwiki.apache.org/confluence/display/WW/S2-073	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-2026-74316	7,5	nfsd4_drop_re-voked_stid() nfsd4_drop_re-voked_stid()		1e33e1414bec54a4feafa9e67e2617031be0afe2 prior to 7ed62f7040ee182cf7dea5798f9e114235b31dae; 1e33e1414bec54a4feafa9e67e2617031be0afe2 prior to da6f86ff4f2dd490bea52419a49e19680efd5847; 1e33e1414bec54a4feafa9e67e2617031be0afe2 prior to 8024028ef91616cf91cc669f2446a0406bc0ba19; 1e33e1414bec54a4feafa9e67e2617031be0afe2 prior to 86b9898920a6d02b4149f4fef9efd77b8aa3b9ca; 6.9	https://git.kernel.org/stable/c/7ed62f7040ee182cf7dea5798f9e114235b31dae https://git.kernel.org/stable/c/8024028ef91616cf91cc669f2446a0406bc0ba19 https://git.kernel.org/stable/c/86b9898920a6d02b4149f4fef9efd77b8aa3b9ca https://git.kernel.org/stable/c/da6f86ff4f2dd490bea52419a49e19680efd5847			
CVE-2026-74365	7,3	BTT lane acquisition BTT lanes serialize access to per-lane metadata and work-space state during BTT I/O		f23859748e3d530217b197e146a9ac84faf0a282 prior to fd7a97b2514cfc4b4cc067a27dd39bde2a8b1735; 6f50b414f1a0d790f11a6438a3ad6d0577eb2c18 prior to 73e35c1bdfa160b41fdbe204e02325f0687de506; 36c75ce3bd299878fd9b238e9803d3817ddafbf3 prior to 417918783bcfe0be135019df16a267b3af442efd; 36c75ce3bd299878fd9b238e9803d3817ddafbf3 prior to 5c53406098b599c420b031e6ec5ba8a2f3794c50; 36c75ce3bd299878fd9b238e9803d3817ddafbf3 prior to 4eafa810b042d985ec6bbf5b514414e73cee6f6f; 36c75ce3bd299878fd9b238e9803d3817ddafbf3 prior to 8d4b989d9c9afe5f185aa5853b666fc4617afe9e; 2577fece583c7c05cda7ad50dde7638c962665e1; 40ba3fa21250e361bdd8f00800b3e2cb6160de95; b0e7a935739f33ed2bd6868b89f97dd4c2683c26; 66eb7b7f23dd9aec5356e7054dd3596ae7648ff5; b27751fb1f271bbb78d5993c0b10011628e40e18; 6.1.63 prior to 6.1.178; 6.6.2 prior to 6.6.145; 4.19.299 prior to 4.20; 5.4.261 prior to 5.5; 5.10.201 prior to 5.11; 5.15.139 prior to 5.16; 6.5.12 prior to 6.6; 6.7	https://git.kernel.org/stable/c/417918783bcfe0be135019df16a267b3af442efd https://git.kernel.org/stable/c/4eafa810b042d985ec6bbf5b514414e73cee6f6f https://git.kernel.org/stable/c/5c53406098b599c420b031e6ec5ba8a2f3794c50 https://git.kernel.org/stable/c/73e35c1bdfa160b41fdbe204e02325f0687de506 https://git.kernel.org/stable/c/8d4b989d9c9afe5f185aa5853b666fc4617afe9e https://git.kernel.org/stable/c/fd7a97b2514cfc4b4cc067a27dd39bde2a8b1735			
CVE-2026-10734	7,2	The Infility Global plugin for WordPress	Improper Neutraliza-tion of Input During Web Page Genera-tion ('Cross-site Scripting')	up to, and including, 2.15.21	https://plugins.trac.wordpress.org/browser/infility-global/trunk/include/InfilityGlobalErrorRecord.php#L25 https://plugins.trac.wordpress.org/browser/infility-global/trunk/include/InfilityGlobalErrorRecord.php#L320 https://plugins.trac.wordpress.org/browser/infility-global/trunk/include/InfilityGlobalErrorRecord.php#L410 https://plugins.trac.wordpress.org/browser/infility-global/trunk/include/InfilityGlobalErrorRecord.php#L414 https://www.wordfence.com/threat-intel/vulnerabilities/id/0de639a9-37a6-4a72-8afb-ff43de81a83c?source=cve			
CVE-2026-13360	7,2	The Cookie Banner for GDPR / CCPA – WPLP Cookie Con-sent plugin for Word-Press	Improper Neutraliza-tion of Input During Web Page Genera-tion ('Cross-site Scripting')	up to, and including, 4.3.5	https://plugins.trac.wordpress.org/browser/gdpr-cookie-consent/tags/4.2.7/admin/class-gdpr-cookie-consent-admin.php#L4961 https://plugins.trac.wordpress.org/browser/gdpr-cookie-consent/tags/4.2.7/includes/class-gdpr-cookie-consent.php#L245 https://plugins.trac.wordpress.org/browser/gdpr-cookie-consent/tags/4.2.7/public/class-gdpr-cookie-consent-public.php#L209 https://plugins.trac.wordpress.org/browser/gdpr-cookie-consent/tags/4.3.5/admin/class-gdpr-cookie-consent-admin.php#L4961 https://plugins.trac.wordpress.org/browser/gdpr-cookie-consent/tags/4.3.5/includes/class-gdpr-cookie-consent.php#L245 https://plugins.trac.wordpress.org/browser/gdpr-cookie-consent/tags/4.3.5/public/class-gdpr-cookie-consent-public.php#L209			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-13424	7,2	The Online Scheduling and Appointment Booking System – Bookly plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 27.7	https://plugins.trac.wordpress.org/browser/bookly-responsive-appointment-booking-tool/tags/27.5/backend/modules/diagnostics/Ajax.php#L344 https://plugins.trac.wordpress.org/browser/bookly-responsive-appointment-booking-tool/tags/27.5/backend/modules/diagnostics/resources/js/diagnostics.js#L542 https://plugins.trac.wordpress.org/browser/bookly-responsive-appointment-booking-tool/tags/27.5/lib/PluginsUpdater.php#L13 https://plugins.trac.wordpress.org/browser/bookly-responsive-appointment-booking-tool/tags/27.5/lib/PluginsUpdater.php#L97 https://plugins.trac.wordpress.org/browser/bookly-responsive-appointment-booking-tool/tags/27.7/backend/modules/diagnostics/Ajax.php#L344 https://plugins.trac.wordpress.org/browser/bookly-responsive-appointment-booking-tool/tags/27.7/backend/modules/diagnostics/resources/js/diagnostics.js#L542	none	yes	partial
CVE-2026-14433	7,2	The Online Booking & Scheduling Calendar for WordPress by vcita plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 4.6.0	https://plugins.trac.wordpress.org/browser/meeting-scheduler-by-vcita/tags/4.6.0/vcita-api-functions.php#L17 https://plugins.trac.wordpress.org/browser/meeting-scheduler-by-vcita/tags/4.6.0/vcita-api-functions.php#L83 https://plugins.trac.wordpress.org/browser/meeting-scheduler-by-vcita/tags/4.6.0/vcita-scheduler.php#L379 https://plugins.trac.wordpress.org/browser/meeting-scheduler-by-vcita/tags/4.6.0/vcita-widgets-functions.php#L22 https://www.wordfence.com/threat-intel/vulnerabilities/id/3fbfb185-d901-4789-9a13-137f72234ed4?source=cve			
CVE-2026-15002	7,2	The Platnosci Online Blue Media (Autopay) plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 5.0.0	https://plugins.trac.wordpress.org/browser/platnosci-online-blue-media/tags/5.0.0/src/Domain/Service/Custom_Styles/Css_Editor.php#L96 https://plugins.trac.wordpress.org/browser/platnosci-online-blue-media/tags/5.0.0/src/Domain/Service/Custom_Styles/Css_Editor.php#L98 https://plugins.trac.wordpress.org/browser/platnosci-online-blue-media/tags/5.0.0/src/Domain/Service/Custom_Styles/Css_Frontend.php#L17 https://plugins.trac.wordpress.org/browser/platnosci-online-blue-media/tags/5.0.0/src/Domain/Service/Settings/Settings_Manager.php#L94 https://plugins.trac.wordpress.org/changeset?reponame=&old=3636306%40platnosci-online-blue-media&new=3636306%40platnosci-online-blue-media https://www.wordfence.com/threat-intel/vulnerabilities/id/f49ccf0f-99ec-410f-8bf0-2f15d8fd578f?source=cve	none	yes	partial
CVE-2026-16145	7,2	The Invisible Anti-Spam & CAPTCHA — reCAPTCHA Alternative for All Forms plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 5.1	https://plugins.trac.wordpress.org/browser/gdpr-compliant-recaptcha-for-all-forms/tags/5.0/includes/class-message-page.php#L621 https://plugins.trac.wordpress.org/browser/gdpr-compliant-recaptcha-for-all-forms/tags/5.0/includes/class-stamp.php#L136 https://plugins.trac.wordpress.org/browser/gdpr-compliant-recaptcha-for-all-forms/tags/5.0/includes/class-stamp.php#L771 https://plugins.trac.wordpress.org/changeset/3633500/gdpr-compliant-recaptcha-for-all-forms https://www.wordfence.com/threat-intel/vulnerabilities/id/ff1d2bd8-cc46-4763-8ba7-832b982ff56a?source=cve			
CVE-2026-17533	7,2	The All-in-One WP Migration and Backup WordPress plugin	Improper Privilege Management	before 7.108	https://wpscan.com/vulnerability/13b57cdc-d954-4db6-94c2-53ad04ab0d34/	poc	no	total

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-17581	7,2	The WCPOS – Point of Sale (POS) plugin for WooCommerce plugin for WordPress	Improper Control of Generation of Code ('Code Injection')	up to, and including, 1.9.14	https://plugins.trac.wordpress.org/browser/woocommerce-pos/tags/1.9.10/includes/Admin/Templates/Single_Template.php#L456 https://plugins.trac.wordpress.org/browser/woocommerce-pos/tags/1.9.10/includes/Services/Receipt_Renderer_Factory.php#L25 https://plugins.trac.wordpress.org/browser/woocommerce-pos/tags/1.9.10/includes/Templates.php#L238 https://plugins.trac.wordpress.org/browser/woocommerce-pos/tags/1.9.10/includes/Templates/Receipt.php#L251 https://plugins.trac.wordpress.org/browser/woocommerce-pos/tags/1.9.10/includes/Templates/Renderers/Legacy_Php_Renderer.php#L42 https://plugins.trac.wordpress.org/browser/woocommerce-pos/tags/1.9.11/includes/Admin/Templates/Single_Template.php#L456	none	no	total
CVE-2026-18653	7,2	The WP Directory Kit WordPress plugin	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	before 1.5.7	https://wpscan.com/vulnerability/e064c261-bc7b-4605-8da7-c7036fc396fc/	poc	no	total
CVE-2026-2497	7,2	The Gallery by Best-WebSoft plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to, and including, 4.7.9.	https://plugins.trac.wordpress.org/browser/gallery-plugin/tags/4.7.6/gallery-plugin.php#L1052 https://plugins.trac.wordpress.org/browser/gallery-plugin/tags/4.7.6/includes/class-gllr-media-table.php#L58 https://plugins.trac.wordpress.org/browser/gallery-plugin/trunk/gallery-plugin.php#L1052 https://plugins.trac.wordpress.org/browser/gallery-plugin/trunk/includes/class-gllr-media-table.php#L58 https://plugins.trac.wordpress.org/changeset?reponame=&old=3609291%40gallery-plugin&new=3609291%40gallery-plugin https://www.wordfence.com/threat-intel/vulnerabilities/id/884b97b7-d023-4752-81b1-086ab022f85e?source=cve	none	no	total
CVE-2026-75091	7,2	The Quill Forms | Conversational Multi Step Forms, Surveys & quizzes plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 5.7.1	https://patchstack.com/database/wordpress/plugin/quillforms/vulnerability/wordpress-quill-forms-plugin-5-7-1-cross-site-scripting-xss-vulnerability https://www.wordfence.com/threat-intel/vulnerabilities/id/7ae927b1-401f-4227-9d50-4adde8e95f24?source=cve			

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-2025-62593 Ray-Project Ray Code Injection Vulnerability	https://cisa.gov/news-events/alerts/2026/08/17/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
Windows 11 File Explorer Gets Faster, Customizable Right-Click Menu With App Extension Controls	https://cybersecuritynews.com/windows-11-file-explorer-gets-faster
Privacy Policy	https://cybersecuritynews.com/privacy-policy-2
Hacker claims 3.6 million Azure account records stolen from major companies	https://bleepingcomputer.com/news/security/hacker-claims-36-million-azure-account-records-stolen-from-major-companies
OpenMatter Network to Take Verification Message to Belgrade Blockchain Week 2026	https://cybersecuritynews.com/openmatter-network-belgrade-blockchain-week-2026
GitHub Outage Disrupts Developers Worldwide Amid Ongoing Investigation	https://cybersecuritynews.com/github-outage-worldwide
Microsoft confirms GitHub is down worldwide	https://bleepingcomputer.com/news/microsoft/microsoft-confirms-github-is-down-worldwide
Windows Server 2022 reaches end of mainstream support in 60 days	https://bleepingcomputer.com/news/microsoft/windows-server-2022-reaches-end-of-mainstream-support-in-60-days
Irregular Details How a Naming Error Let AI Models Attack a Real Company	https://securityweek.com/irregular-details-how-a-naming-error-let-ai-models-attack-a-real-company
How MCP Servers Can Expose Enterprise Secrets	https://thehackernews.com/2026/08/how-mcp-servers-can-expose-enterprise.html
Threema Secure Messaging Service Hit by Massive DDoS Attack	https://cybersecuritynews.com/threema-hit-by-massive-ddos-attack
ETSI Proposes 17 Cybersecurity Standards to Support EU CRA	https://infosecurity-magazine.com/news/etsi-proposes-17-cybersecurity
Why Your AI Developer Tools Might Be Your Biggest Security Risk	https://thehackernews.com/expert-insights/2026/08/why-your-ai-developer-tools-might-be.html
The Long Road From Pentest Finding to Verified Fix	https://thehackernews.com/expert-insights/2026/08/the-long-road-from-pentest-finding-to.html
Identity Governance Wasn't Built for Breaches That Happen in Hours	https://thehackernews.com/expert-insights/2026/08/identity-governance-wasnt-built-for.html
Z.ai Unveils GLM-5.3 with Major Enhancements for Coding and Cybersecurity	https://cybersecuritynews.com/glm-5-3-major-enhancements
Infostealers Harvest 1.7 Billion Credentials in Six Months	https://infosecurity-magazine.com/news/infostealers-17-billion
Fortune 500 Companies Hit in Azure Data Theft Campaign	https://securityweek.com/fortune-500-companies-hit-in-azure-data-theft-campaign
Anthropic confirms Claude is down in major outage affecting multiple services	https://bleepingcomputer.com/news/artificial-intelligence/anthropic-confirms-claude-is-down-in-major-outage-affecting-multiple-services
Large-scale DDoS attacks disrupted Threema secure messaging service	https://bleepingcomputer.com/news/security/large-scale-ddos-attacks-disrupted-threema-secure-messaging-service
Microsoft Begins to Merge Consumer and Enterprise Copilot Apps to Make New Super App	https://cybersecuritynews.com/microsoft-combines-copilot-apps

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
Pokémon Center Confirms Data Breach - Hackers Stole Customers' Personal Data	https://cybersecuritynews.com/pokemon-center-confirms-data-breach
Pokémon Center data breach exposes customer info, cancels some orders	https://bleepingcomputer.com/news/security/pokemon-center-data-breach-exposes-customer-info-cancels-some-orders
680,000 Impacted by French Tax Authority Data Breach	https://securityweek.com/680000-impacted-by-french-tax-authority-data-breach
French tax authority data breach affects 678,000 individuals	https://bleepingcomputer.com/news/security/french-tax-authority-data-breach-affects-678-000-individuals
40,000 Impacted by SafePal Data Breach	https://securityweek.com/40000-impacted-by-safepal-data-breach
SafePal Data Breach Hits Tens of Thousands of Customers	https://infosecurity-magazine.com/news/safepal-data-breach-tens-thousands
SafePal data breach impacts 39,798 customers, stolen info for sale	https://bleepingcomputer.com/news/security/safepal-data-breach-impacts-39-798-customers-stolen-info-for-sale
Shell Investigating Data Breach Following Cl0p Ransomware Group Claim	https://cybersecuritynews.com/shell-investigating-data-breach

Vulnerabilities / Flaws / Zero-day

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

Σύντομη περιγραφή / Τίτλος	URL
CISA Flags Actively Exploited Ray Flaw That Can Trigger Browser-Based RCE	https://thehackernews.com/2026/08/cisa-flags-actively-exploited-ray-flaw.html
Public Exploit Code Released for Microsoft SCCM Remote Code Execution Vulnerability	https://cybersecuritynews.com/microsoft-sccm-vulnerability-poc-release
Critical GitLab GraphQL Flaw Could Let Unauthenticated Attackers Delete Public Projects	https://thehackernews.com/2026/08/critical-gitlab-graphql-flaw-could-let.html
Snowflake GitHub Actions Flaw Lets Crafted Issues Trigger Command Injection	https://thehackernews.com/2026/08/snowflake-github-actions-flaw-lets_0330881554.html
Forminator WordPress Flaw Can Enable Unauthenticated RCE via Malicious PHP Uploads	https://thehackernews.com/2026/08/forminator-wordpress-flaw-can-enable.html
UNISOC Modem Flaw Enables Remote Code Execution via Video Calls	https://infosecurity-magazine.com/news/unisoc-modem-flaw-rce-calls
WordPress Plugin Flaw Exposes 40,000 Sites to Admin Takeover	https://infosecurity-magazine.com/news/wordpress-plugin-flaw-40000-sites
Weekly Recap: VMware Exploits, Windows 0-Day, MCP Attacks, Browser Hijacks and More	https://thehackernews.com/2026/08/weekly-recap-vmware-exploits-windows-0.html

Σύντομη περιγραφή / Τίτλος	URL
Microsoft SCCM Vulnerability Chained to Execute Malicious Code Remotely	https://cybersecuritynews.com/microsoft-sccm-vulnerability
Roundcube 1.6.18 and 1.7.3 Released With Fix for RCE and SSRF Vulnerabilities	https://cybersecuritynews.com/roundcube-1-6-18-and-1-7-3-released-with-fix
Unisoc VoLTE Video Call Exploit Chain Can Give Attackers Full Android Kernel Access	https://thehackernews.com/2026/08/unisoc-volte-video-call-exploit-chain.html
Microsoft working on Defender patch for ShieldBreak zero-day	https://bleepingcomputer.com/news/security/microsoft-working-on-defender-patch-for-shieldbreak-zero-day
Recent macOS Screen Sharing Vulnerability Exploited in Attacks	https://securityweek.com/recent-macos-screen-sharing-vulnerability-exploited-in-attacks
Critical SAP Commerce Cloud Vulnerability Exploited 3 Days After Disclosure	https://securityweek.com/critical-sap-commerce-cloud-vulnerability-exploited-3-days-after-disclosure
Apple Screen Sharing Vulnerability Exploited to Execute Command as Root	https://cybersecuritynews.com/apple-screen-sharing-vulnerability
Cyber Security Weekly Newsletter – Outlook RCE, Palo Alto, Cisco 0-day and Windows 0-Day Flaws +20 Stories	https://cybersecuritynews.com/cyber-security-weekly-newsletter-august
SAP Commerce Cloud CVE-2026-58231 Targeted in Exploitation Attempts Days After Patch	https://thehackernews.com/2026/08/sap-commerce-cloud-cve-2026-58231.html
Apple macOS Screen Sharing Flaw Exploited on Internet-Exposed Macs to Install Monero Miner	https://thehackernews.com/2026/08/apple-macos-screen-sharing-flaw.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
Dozens of WebKit Vulnerabilities Patched With Fresh macOS, iOS Security Updates	https://securityweek.com/dozens-of-webkit-vulnerabilities-patched-with-fresh-macos-ios-security-updates

Potential threats / Threat intelligence

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

Σύντομη περιγραφή / Τίτλος	URL
Claude Code Helps Ransomware Operator Steal LDAP Passwords, Backdoor VPNs and Exfiltrate SQL Databases	https://cybersecuritynews.com/claude-code-helps-ransomware-operator
Turf War Between Claude Agents Leads to Self-Replicating Malware	https://darkreading.com/threat-intelligence/turf-war-claude-agents-self-replicating-malware
Philips and GE investigating Clop ransomware data theft claims	https://bleepingcomputer.com/news/security/philips-and-ge-investigating-clop-ransomware-data-theft-claims
Conflicting Test Goals Pushed Claude Agents to Deploy Self-Replicat-ing Malware	https://securityweek.com/conflicting-test-goals-pushed-claude-agents-to-deploy-self-replicating-malware
Evooo1Bot Linux Botnet Exploits Known Flaws to Turn Edge Devices Into SOCKS5 Proxies	https://thehackernews.com/2026/08/evooo1bot-linux-botnet-exploits-known.html
HoneyMyte CoolClient Backdoor Uses Signed Kernel Rootkit to Hide Processes, Files and C2 Traffic	https://cybersecuritynews.com/honeymyte-coolclient-backdoor
Suspected China-Nexus Actor Exploits VMware vCenter Flaw, Deploys Babuk-Derived Ransomware	https://thehackernews.com/2026/08/suspected-china-nexus-actor-exploits.html
New MessiahGPT AI Model Fueling Automated Ransomware and Phish-ing Attacks	https://cybersecuritynews.com/messiahgpt-fueling-ransomware-phishing-attacks
ChainDrop npm Worm Poisons 444 Packages Through GitHub Actions and Trusted Publishing	https://cybersecuritynews.com/chaindrop-npm-worm
12 KB Windows Backdoor Hides C2 Domain in desktop.ini Whitespace to Evade Detection	https://cybersecuritynews.com/12-kb-windows-backdoor
New AmnesiaStealer macOS malware hijacks browser sessions via re-mote control	https://bleepingcomputer.com/news/security/new-amnesiastealer-macos-malware-hijacks-browser-sessions-via-remote-control
McDonald's, Vodafone Hit by Azure Credential Theft Campaign Expos-ing Millions of Enterprise Records	https://cybersecuritynews.com/azure-credential-theft-campaign
New Evooo1Bot Linux botnet turns routers into traffic relay nodes	https://bleepingcomputer.com/news/security/new-evooo1bot-linux-botnet-turns-routers-into-traffic-relay-nodes

Guides / Tools

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

Σύντομη περιγραφή / Τίτλος	URL
Top 10 Best Network Sandboxing Solutions in 2026	https://cybersecuritynews.com/best-network-sandboxing-solutions
Top 10 Best Software-Defined Perimeter (SDP) Solutions in 2026	https://cybersecuritynews.com/best-software-defined-perimeter-solutions

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 15/08/2026–18/08/2026 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/