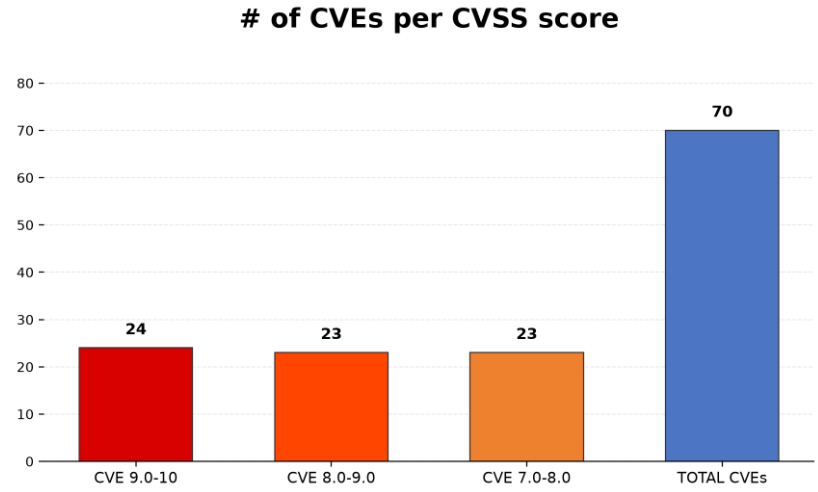
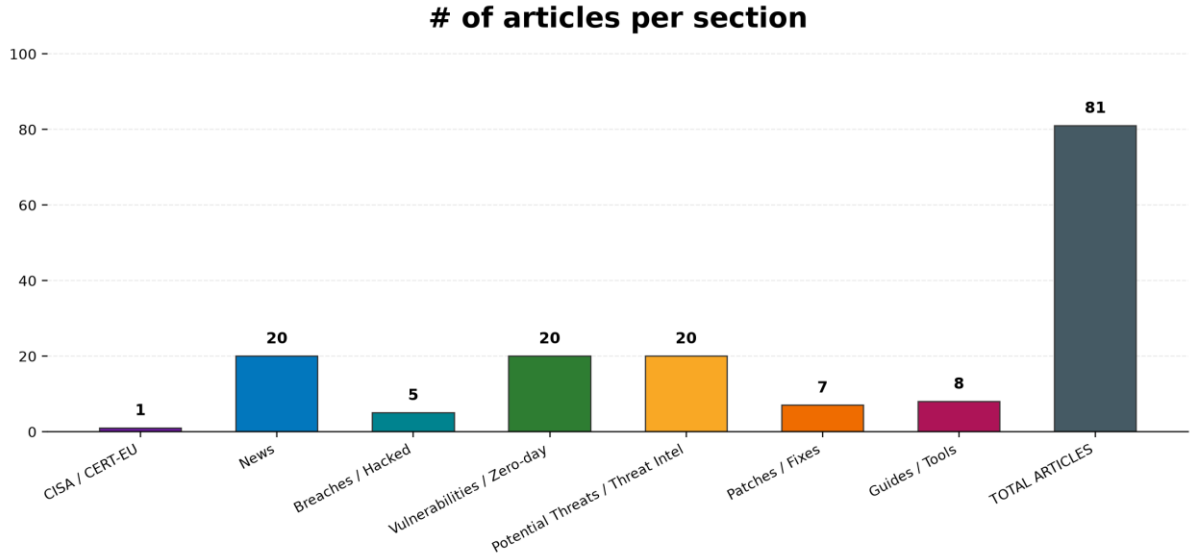
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 05/08/2026 - 07/08/2026





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-2026-16940	10,0	The Custom Fields WordPress plugin	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	before 1.5.1	https://wpscan.com/vulnerability/a315a6ac-3ffb-4735-92ca-6e85338f8807/	none	yes	total
CVE-2026-48168	10,0	PraisonAI	Missing Authorization	versions prior to 4.6.40	https://github.com/MervinPraison/PraisonAI/commit/179cab02dbec0c1e9b601507a659 https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-xp85-6wwf-r67c	poc	yes	total
CVE-2026-56162	10,0	Azure SQL Database	Improper Authentication		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56162	none	yes	total
CVE-2026-63508	10,0	Microsoft Planetary Computer Pro	Missing Authentication for Critical Function		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-63508			
CVE-2026-65553	10,0	Spider Analyser – WordPress搜索引擎蜘蛛分析插件	Improper Control of Generation of Code ('Code Injection')	<= 2.1.3	https://patchstack.com/database/wordpress/plugin/spider-analyser/vulnerability/wordpress-spider-analyser-wordpress-plugin-2-1-3-remote-code-execution-rce-vulnerability?_s_id=cve	none	yes	total
CVE-2026-65667	10,0	Microsoft Teams	Missing Authorization		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65667	none	yes	total
CVE-2026-66665	10,0	Type Hub	Unrestricted Upload of File with Dangerous Type	<= 2.0.6	https://patchstack.com/database/wordpress/plugin/typehub/vulnerability/wordpress-type-hub-plugin-2-0-6-arbitrary-file-upload-vulnerability?_s_id=cve	none	yes	total
CVE-2026-48086	9,9	OpenReception's appointment booking software	Improper Privilege Management	Prior to version 1.0.2	https://github.com/open-reception/appointment-booking-software/commit/8525d35a41c31078d9f01c62e9687e653cf1a494 https://github.com/open-reception/appointment-booking-software/security/advisories/GHSA-5qfr-7q4g-3469			
CVE-2026-50481	9,9	Azure Active Directory	Modification of Assumed-Immutable Data (MAID)		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50481	none	no	total
CVE-2026-50515	9,9	Azure Service Bus	Deserialization of Untrusted Data		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50515			
CVE-2026-62830	9,9	Azure SRE Agent	Missing Authorization		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62830			
CVE-2026-65548	9,9	Betheme	Improper Control of Generation of Code ('Code Injection')	<= 28.4.2	https://patchstack.com/database/wordpress/theme/betheme/vulnerability/wordpress-betheme-theme-28-4-2-remote-code-execution-rce-vulnerability?_s_id=cve	none	no	total
CVE-2026-67622	9,9	Flowise	Authorization Bypass Through User-Controlled Key	through 3.1.4	https://flowiseai.com/sunset https://github.com/Caycon/cve-advisories/blob/main/2026/Flowise/CVE-2026-67622.md			
CVE-2026-70615	9,9	boringproxy	Improper Neutralization of CRLF Sequences ('CRLF Injection')	through 0.10.0	https://github.com/theopaid/Remote-Code-Execution-And-Privilege-Escalation-Through-SSH-Authorized-Keys-Injection-boringproxy-/blob/master/README.md https://www.vulncheck.com/advisories/boringproxy-ssh-authorized-keys-injection-via-tunnel-creation	poc	no	partial

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-71268	9,9	OpenPLC_v3	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')		https://github.com/thiagoralves/OpenPLC_v3 https://github.com/thiagoralves/OpenPLC_v3/blob/master/webserver/openplc.py	none	no	total
CVE-2026-7329	9,9	the SQL, SPARQL, and Optic REST query interfaces of Progress MarkLogic Server	Improper Privilege Management	before 11.3.6 and 12.0.3	https://community.progress.com/s/article/Marklogic-Critical-Security-Alert-Bulletin-August-2026	none	no	total
CVE-2026-8709	9,9	the REST API document patch operation of Progress MarkLogic Server	Improper Privilege Management	before 11.3.6 and 12.0.3	https://community.progress.com/s/article/Marklogic-Critical-Security-Alert-Bulletin-August-2026	none	no	total
CVE-2026-9193	9,9	the Hadoop integration of Progress MarkLogic Server	Improper Privilege Management	before 11.3.6 and 12.0.3	https://community.progress.com/s/article/Marklogic-Critical-Security-Alert-Bulletin-August-2026	none	no	total
CVE-2025-63823	9,8	My Safetipin Android Application	Use of Hard-coded Credentials		https://github.com/Leoccc98/cve-reports/blob/main/advisories/CVE-2025-63823/README.md https://play.google.com/store/apps/details?id=com.safetipin.mysafetipin	none	yes	total
CVE-2026-14364	9,8	The TrueBooker – Appointment Booking and Scheduler System plugin for WordPress	Weak Password Recovery Mechanism for Forgotten Password	up to, and including, 1.2.3.	https://plugins.trac.wordpress.org/changeset/3595807/truebooker-appointment-booking https://www.wordfence.com/threat-intel/vulnerabilities/id/f441477e-35b8-42ae-b71c-3fdba126021b?source=cve			
CVE-2026-28005	9,8	Kadence WooCommerce Email Designer	Missing Authorization	<= 1.5.19	https://patchstack.com/database/wordpress/plugin/kadence-woocommerce-email-designer/vulnerability/wordpress-kadence-woocommerce-email-designer-plugin-1-5-19-privilege-escalation-vulnerability?_s_id=cve	none	yes	total
CVE-2026-28139	9,8	Ajax Search Lite	Deserialization of Untrusted Data	<= 4.14.4	https://patchstack.com/database/wordpress/plugin/ajax-search-lite/vulnerability/wordpress-ajax-search-lite-plugin-4-14-4-php-object-injection-vulnerability?_s_id=cve	none	yes	total
CVE-2026-45538	9,8	OpenSIPS	Stack-based Buffer Overflow	In versions 4.0.0 and prior	https://github.com/OpenSIPS/opensips/security/advisories/GHSA-37wc-5j8j-95x3	poc	yes	total
CVE-2026-52466	9,8	Open Library Foundation VuFind	Incorrect Authorization		https://vufind.org/wiki/security:cve-2026-52466	none	yes	total
CVE-2026-15991	8,8	The File Manager plugin for WordPress	Missing Authorization	6.0 through 6.9	https://plugins.trac.wordpress.org/browser/file-manager/tags/6.9/backend/app/Http/Controllers/FileManagerController.php#L32 https://plugins.trac.wordpress.org/browser/file-manager/tags/6.9/backend/app/Http/Controllers/FileManagerController.php#L34 https://plugins.trac.wordpress.org/browser/file-manager/tags/6.9/backend/app/Providers/AccessControlProvider.php#L121 https://plugins.trac.wordpress.org/browser/file-manager/tags/6.9/backend/hooks/ajax.php#L10 https://plugins.trac.wordpress.org/browser/file-manager/tags/6.9/vendor/studio-42/elfinder/php/elFinder.class.php#L802 https://plugins.trac.wordpress.org/browser/file-manager/tags/6.9/vendor/studio-42/elfinder/php/elFinderConnector.class.php#L320	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-2026-18258	8,8	the Line, LineTranscription, VirtualCollection, tag and process API endpoints in Scripta/eScriptorium	Authorization Bypass Through User-Controlled Key	through 26.04.1	https://gitlab.com/scripta/escriptorium/-/work_items/1226	none	no	total
CVE-2026-18322	8,8	The Smart Popup by Supsystic plugin for WordPress; all	Improper Privilege Management	up to, and including, 1.12.0.	https://plugins.trac.wordpress.org/browser/popup-by-supsystic/tags/1.11.2/classes/frame.php#L180 https://plugins.trac.wordpress.org/browser/popup-by-supsystic/tags/1.11.2/modules/popup/models/popup.php#L316 https://plugins.trac.wordpress.org/browser/popup-by-supsystic/tags/1.11.2/modules/subscribe/models/subscribe.php#L292 https://plugins.trac.wordpress.org/browser/popup-by-supsystic/tags/1.11.2/modules/subscribe/models/subscribe.php#L358 https://plugins.trac.wordpress.org/browser/popup-by-supsystic/tags/1.11.2/modules/subscribe/models/subscribe.php#L440 https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3629986%40popup-by-supsystic%2Ftrunk%2Fmodules%2Fsubscribe%2Fmodels%2Fsubscribe.php&old=3628131%40popup-by-supsystic%2Ftrunk%2Fmodules%2Fsubscribe%2Fmodels%2Fsubscribe.php&sfp_email=&sfph_mail=	none	no	total
CVE-2026-18895	8,8	UTT HiPER	Improper Restriction of Operations within the Bounds of a Memory Buffer; Stack-based Buffer Overflow	up to 3.2.7-210907-180535.	https://github.com/7wkajk/CVE-VUL/blob/main/101.md https://vuldb.com/cve/CVE-2026-18895 https://vuldb.com/submit/858607 https://vuldb.com/vuln/385930 https://vuldb.com/vuln/385930/cti	poc	no	total
CVE-2026-19145	8,8	Translate in Google Chrome	Use After Free	prior to 151.0.7922.109	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_01193673229.html https://issues.chromium.org/issues/521878431	none	no	total
CVE-2026-19150	8,8	V8 in Google Chrome	Protection Mechanism Failure	prior to 151.0.7922.109	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_01193673229.html https://issues.chromium.org/issues/526380803	none	no	total
CVE-2026-19169	8,8	Contextual Tasks in Google Chrome	Improper Input Validation	prior to 151.0.7922.109	https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_01193673229.html https://issues.chromium.org/issues/537390933	none	no	total
CVE-2026-28111	8,8	Forminator	Incorrect Privilege Assignment	<= 1.56.0	https://patchstack.com/database/wordpress/plugin/forminator/vulnerability/wordpress-forminator-plugin-1-56-0-privilege-escalation-vulnerability?_s_id=cve	none	no	total
CVE-2026-49163	8,8	Application Insights Profiler	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-49163			
CVE-2026-55997	8,8	rancher	Cleartext Storage of Sensitive Information	2.14.0 prior to 2.14.4; 2.13.0 prior to 2.13.8	https://bugzilla.suse.com/show_bug.cgi?id=CVE-2026-55997 https://github.com/rancher/rancher/security/advisories/GHSA-7r53-jvhg-9jg4	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-2026-6147	8,8	The LightSync Pro plugin for Word-Press	Unrestricted Upload of File with Dangerous Type	up to, and including, 2.1.6.	https://plugins.trac.wordpress.org/browser/lightsyncpro/tags/2.0.1/includes/admin/class-admin.php#L6755 https://plugins.trac.wordpress.org/browser/lightsyncpro/tags/2.0.1/includes/admin/class-admin.php#L6814 https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3507389%40lightsyncpro%2Ftrunk&old=3476495%40lightsyncpro%2Ftrunk&sfp_email=&sfph_mail= https://www.wordfence.com/threat-intel/vulnerabilities/id/9ccdf08b-8b74-4b58-8779-3b07ef2d7b2f?source=cve	none	no	total
CVE-2026-65542	8,8	Super Socializer	Authentication Bypass Using an Alternate Path or Channel	<= 7.14.5	https://patchstack.com/database/wordpress/plugin/super-socializer/vulnerability/wordpress-super-socializer-plugin-7-14-5-broken-authentication-vulnerability?_s_id=cve	none	no	total
CVE-2026-65668	8,8	Microsoft Purview eDiscovery	Improper Access Control		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65668	none	no	total
CVE-2026-67623	8,8	Mistral Vibe	Inclusion of Functionality from Untrusted Control Sphere	before 2.23.3	https://github.com/mistralai/mistral-vibe/commit/68ff32e6a92e80a874c8153312f0aa8ae4955477 https://github.com/mistralai/mistral-vibe/issues/942 https://github.com/mistralai/mistral-vibe/pull/962 https://github.com/mistralai/mistral-vibe/pull/978 https://github.com/mistralai/mistral-vibe/releases/tag/v2.23.3 https://therealcoiffeur.com/c111011.html	none	no	total
CVE-2026-70374	8,8	HashBrown CMS	Improper Neutralization of Special Elements used in an OS Command ('OS Com-mand Injection')	through 1.4.6	https://cve.turansec.uz/advisories/TRN-11FC0D88 https://github.com/HashBrownCMS/hashbrown-cms	none	no	total
CVE-2026-70431	8,8	Jenkins Multijob Plugin	Improper Control of Genera-tion of Code ('Code Injec-tion')	669.v9d96a_d9c71b_0 and earlier	https://www.jenkins.io/security/advisory/2026-08-05/#SECURITY-3823%20(1)	none	no	total
CVE-2026-70619	8,8	Odysseus before commit bf325f6	Missing Authorization	prior to bf325f6b2185cb42bc5d8f5713a64aecffb766d4	https://aydinnyunus.github.io/2026/06/16/odysseus-embedding-endpoint-takeover/ https://github.com/odysseus-dev/odysseus/commit/bf325f6b2185cb42bc5d8f5713a64aecffb766d4 https://github.com/odysseus-dev/odysseus/issues/132 https://github.com/odysseus-dev/odysseus/issues/80 https://www.vulncheck.com/advisories/odysseus-missing-admin-authorization-via-embedding-endpoint-routes	poc	no	total
CVE-2026-71235	8,8	Magistrala's Rules Engine	Improper Control of Genera-tion of Code ('Code Injec-tion')		https://github.com/absmach/magistrala	none	no	total
CVE-2026-71243	8,8	backmeup	Improper Neutralization of Special Elements used in an OS Command ('OS Com-mand Injection')	0.0.2 and earlier	https://github.com/adaltas/node-backmeup	none	no	total
CVE-2026-71281	8,8	peft	Deserialization of Untrusted Data	0.19.1 and earlier	https://github.com/huggingface/peft https://github.com/huggingface/peft/blob/main/src/peft/tuners/lora/corda.py	none	no	total
CVE-2026-71287	8,8	cacti	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injec-tion')	1.3.0-dev and earlier	https://github.com/Cacti/cacti https://github.com/Cacti/cacti/blob/develop/lib/functions.php	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-2026-71288	8,8	Koha	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26.05.01-1 and earlier	https://github.com/Koha-Community/Koha https://github.com/Koha-Community/Koha/blob/master/reports/guided_reports.pl	none	no	total
CVE-2026-71291	8,8	Bolt CMS	Improper Neutralization of Special Elements Used in a Template Engine	6.1 and earlier	https://github.com/bolt/core https://github.com/bolt/core/blob/6.1/src/Entity/Field.php	none	no	total
CVE-2026-12410	7,8	the Uninstaller component in CCleaner	Improper Link Resolution Before File Access ('Link Following')	prior to 7.10.1464	https://www.gendigital.com/us/en/contact-us/security-advisories/	none	no	total
CVE-2026-1289	7,8	A maliciously crafted PDF file, when parsed through Autodesk Revit, can force a	Use After Free	2027.0.0 prior to 2027.2.0; 2026.0.0 prior to 2026.5.0	https://www.autodesk.com/products/autodesk-access/overview https://www.autodesk.com/trust/security-advisories/adsk-sa-2026-0011			
CVE-2026-16022	7,8	@oblique/cli	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	15.4.0 prior to 15.4.2	https://github.com/oblique-bit/oblique/blob/master/projects/cli/CHANGELOG.md	none	no	total
CVE-2026-18485	7,8	There; the NI-PAL kernel driver	Improper Validation of Specified Index, Position, or Offset in Input	26.3	https://www.ni.com/en/support/security/available-critical-and-security-updates-for-ni-software/2026/local-privilege-escalation-in-ni-pal.html	none	no	total
CVE-2026-19189	7,8	Power Sofware PowerISO	Incorrect Privilege Assignment; Improper Privilege Management	9.3.0.0	https://vuldb.com/cve/CVE-2026-19189 https://vuldb.com/submit/864536 https://vuldb.com/vuln/386707 https://vuldb.com/vuln/386707/cti https://winslow1984.com/books/cve-collection/page/poweriso-9300-kernel-driver-6900-local-privilege-escalation-via-arbitrary-registry-write-or-deletion			
CVE-2026-19190	7,8	StableBit Scanner	Incorrect Privilege Assignment; CWE CATEGORY: Permission Issues	2.6.13.4088	https://vuldb.com/cve/CVE-2026-19190 https://vuldb.com/submit/864538 https://vuldb.com/vuln/386708 https://vuldb.com/vuln/386708/cti https://winslow1984.com/books/cve-collection/page/stablebit-scanner-26134088-local-privilege-escalation-via-insecure-deserialization			
CVE-2026-19191	7,8	StableBit DrivePool	Incorrect Privilege Assignment; CWE CATEGORY: Permission Issues	2.3.13.1687	https://vuldb.com/cve/CVE-2026-19191 https://vuldb.com/submit/864539 https://vuldb.com/vuln/386709 https://vuldb.com/vuln/386709/cti https://winslow1984.com/books/cve-collection/page/stablebit-drivepool-23131687-local-privilege-escalation-via-insecure-deserialization			
CVE-2026-19192	7,8	DeepCool DisplayService	Incorrect Privilege Assignment; Improper Access Control	1.2.12	https://vuldb.com/cve/CVE-2026-19192 https://vuldb.com/submit/864540 https://vuldb.com/vuln/386710 https://vuldb.com/vuln/386710/cti https://winslow1984.com/books/cve-collection/page/deepcool-1212-displayservice-exposes-an-unauthenticated-localsystem-named-pipe-control-channel			
CVE-2026-19193	7,8	Jiangmin Antivirus	Incorrect Privilege Assignment; Improper Access Control	21	https://github.com/patrickt2017/research/issues/1 https://vuldb.com/cve/CVE-2026-19193 https://vuldb.com/submit/864551 https://vuldb.com/vuln/386711 https://vuldb.com/vuln/386711/cti			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-19195	7,8	V-Secure Jingyun Antivirus	Incorrect Privilege Assignment; Improper Access Control	2.4.2.39	https://github.com/patrickt2017/research/issues/2 https://vuldb.com/cve/CVE-2026-19195 https://vuldb.com/submit/864561 https://vuldb.com/vuln/386712 https://vuldb.com/vuln/386712/cti			
CVE-2026-70628	7,8	FFmpeg	Integer Overflow or Wraparound; Out-of-bounds Write	0.5 prior to 9.0	https://code.ffmpeg.org/FFmpeg/FFmpeg/commit/02fc47e13f903768b75f7985a2706a6223ab4506 https://code.ffmpeg.org/FFmpeg/FFmpeg/commit/93f2a525ec6c7b467bae68322720d10188fc6e30 https://code.ffmpeg.org/FFmpeg/FFmpeg/commit/c6ec28b18cd1eb7d39e6163137367f2d1c62aa7c https://code.ffmpeg.org/FFmpeg/FFmpeg/pulls/23897			
CVE-2026-71261	7,8	dr_libs	Integer Overflow or Wraparound		https://github.com/mackron/dr_libs https://github.com/mackron/dr_libs/blob/master/dr_wav.h	none	no	total
CVE-2026-71266	7,8	tinyobjloader-c	Stack-based Buffer Overflow	< 4095	https://github.com/syoyo/tinyobjloader-c https://github.com/syoyo/tinyobjloader-c/blob/master/tinyobj_loader_c.h	none	no	total
CVE-2026-7867	7,8	udisks2	Incorrect Authorization		https://access.redhat.com/security/cve/CVE-2026-7867 https://bugzilla.redhat.com/show_bug.cgi?id=2466747 https://github.com/storaged-project/udisks/releases/tag/udisks-2.11.2 https://github.com/storaged-project/udisks/security/advisories/GHSA-j42g-v9jw-6ph3			
CVE-2026-34966	7,6	Gitea	Server-Side Request Forgery (SSRF)	prior to 1.27.0	https://github.com/go-gitea/gitea https://github.com/go-gitea/gitea/commit/b969123b7fac51c88daab5cb64e5b2f4abd53288 https://github.com/go-gitea/gitea/security/advisories/GHSA-2wm4-vwp6-v7xc https://www.vulncheck.com/advisories/gitea-prior-to-ssrf-via-migration-uri-fetch-bypass	poc	no	partial
CVE-2026-71294	7,6	Cotonti	Deserialization of Untrusted Data		https://github.com/Cotonti/Cotonti https://github.com/Cotonti/Cotonti/blob/master/plugins/comments/controllers/actions/CreateAction.php	none	no	partial
CVE-2026-10524	7,5	The CoCart WordPress plugin		before 4.9.0	https://wpscan.com/vulnerability/99986e13-d38d-4890-b935-9f6fd238ec61/			
CVE-2026-10599	7,5	The Integrate PhonePe with WooCommerce WordPress plugin		through 1.2.1	https://wpscan.com/vulnerability/a1aae05d-63d0-4cde-8a9c-996f58f58e48/			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-12000	7,5	The Page and Post Restriction plugin for WordPress	Missing Authorization	up to and including 1.4.0	https://plugins.trac.wordpress.org/browser/page-and-post-restriction/tags/1.4.0/page-and-post-restriction.php#L484 https://plugins.trac.wordpress.org/browser/page-and-post-restriction/tags/1.4.0/page-and-post-restriction.php#L69 https://plugins.trac.wordpress.org/browser/page-and-post-restriction/tags/1.4.0/page-and-post-restriction.php#L94 https://plugins.trac.wordpress.org/browser/page-and-post-restriction/tags/1.4.0/page-restriction-utility.php#L701 https://plugins.trac.wordpress.org/browser/page-and-post-restriction/tags/1.4.1/page-and-post-restriction.php#L484 https://plugins.trac.wordpress.org/browser/page-and-post-restriction/tags/1.4.1/page-and-post-restriction.php#L69	none	yes	partial
CVE-2026-12584	7,5	The Payment Gateway for Redsys & WooCommerce Lite WordPress plugin		before 7.0.2	https://wpscan.com/vulnerability/1ff08062-8f2c-4542-b795-fe82bfa6040c/			
CVE-2026-13153	7,5	The Gutenberg Essential Blocks WordPress plugin	Exposure of Sensitive Information to an Unauthorized Actor	before 6.4.0	https://wpscan.com/vulnerability/0401a229-9630-49ab-ae4b-53360cf5d109/	poc	yes	partial
CVE-2026-13399	7,5	The Payment Plugins for PayPal WooCommerce WordPress plugin		before 2.0.20	https://wpscan.com/vulnerability/6ae19ba0-26ba-4ffa-94e3-3fe32cedcae1/			
CVE-2026-15372	7,5	The WP	Improper Authentication	before 4.1.0	https://wpscan.com/vulnerability/a8d697c9-6de4-4a28-be9e-7d42abcb6c7e/	poc	no	partial

CISA/CERT-EU Alerts & Advisories

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

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds One Known Exploited Vulnerability to Catalog | CISA	▪ CVE-2026-63077 JetBrains TeamCity Deserialization of Untrusted Data Vulnerability	https://cisa.gov/news-events/alerts/2026/08/05/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
Papyrus Mobile Ad Fraud Uses Hidden WebViews to Fake Clicks, Scrolls and Attention	https://cybersecuritynews.com/papyrus-mobile-ad-fraud
Kimi K3 AI Model Escapes Sandbox During Security Test to Fetch Answers	https://cybersecuritynews.com/kimi-k3-ai-model-escapes-sandbox
Privacy Policy	https://cybersecuritynews.com/privacy-policy-2
OpenAI Expands GPT-5.6 Access to Free & Go Users With Unlimited Text Chats	https://cybersecuritynews.com/openai-expands-gpt-5-6-access
OpenAI rolls out a major ChatGPT upgrade, even if you don't pay for it	https://bleepingcomputer.com/news/artificial-intelligence/openai-rolls-out-a-major-chatgpt-upgrade-even-if-you-dont-pay-for-it
The Coordination Gap: How Attackers Are Outpacing Law Enforcement	https://darkreading.com/cyberattacks-data-breaches/coordination-gap-attackers-outpacing-law-enforcement
Researcher Claims Control of ChatGPT Secure Sandbox	https://darkreading.com/cloud-security/researcher-claims-control-chatgpt-secure-sandbox
4,400+ Internet-Exposed Rockwell PLCs Expose Water Systems to Cyberattacks	https://cybersecuritynews.com/internet-exposed-rockwell-plcs
New Interrupt Injection Attack Can Bypass Spectre v2 Defenses on Intel and AMD CPUs	https://thehackernews.com/2026/08/new-interrupt-injection-attack-can.html
Snowflake Hacker Pleads Guilty in US Court	https://securityweek.com/snowflake-hacker-pleads-guilty-in-us-court
Meta Joins OpenAI and Anthropic in Reporting AI Exploit Incident	https://infosecurity-magazine.com/news/meta-ai-exploit-incident
Zero-Click AI Browser Hacking: Claude and ChatGPT Atlas Hijacked via Emails, X Posts	https://securityweek.com/zero-click-ai-browser-hacking-claude-and-chatgpt-atlas-hijacked-via-emails-x-posts
Over 4,400 Rockwell PLCs Exposed Online, 22 Found in Water Attack Cities	https://thehackernews.com/2026/08/over-4400-rockwell-plcs-exposed-online.html
Violent Physical Crypto Thefts Surge to $30m in Losses	https://infosecurity-magazine.com/news/violent-physical-crypto-thefts
Podcast: Compliance Won't Save You: The Future of Cyber Risk with Edna Conway	https://securityweek.com/podcast-compliance-wont-save-you-the-future-of-cyber-risk-with-edna-conway
CryptoJS Weak RNG Behind $5.7 Million in Drains Affects Five Crypto Wallet Apps	https://thehackernews.com/2026/08/cryptojs-weak-rng-behind-57-million-in.html
Apple iCloud Private Relay Can Expose Real IPs Through WebKit Proxy Bypasses	https://thehackernews.com/2026/08/webkit-proxy-bypasses-can-expose-real.html
Canadian Hacker Pleads Guilty Over Snowflake Extortion Campaign	https://infosecurity-magazine.com/news/canadian-hacker-guilty-snowflake
Belarusian Ransom Cartel Mastermind Gets 16 Years in Prison	https://securityweek.com/belarusian-ransom-cartel-mastermind-gets-16-years-in-prison
NVIDIA Group Proposes SAFE Initiative for Agentic Threat Intel Sharing	https://infosecurity-magazine.com/news/safe-initiative-agentic-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
3.8 Million Impacted by Unlimited Technology Systems Data Breach	https://securityweek.com/3-8-million-impacted-by-unlimited-technology-systems-data-breach
Swiss government SharePoint breach compromised 200 accounts	https://bleepingcomputer.com/news/security/swiss-government-sharepoint-breach-compromised-200-accounts
Meta AI model hacked a company during misconfigured cyber test	https://bleepingcomputer.com/news/security/meta-ai-model-hacked-a-company-during-misconfigured-cyber-test
Meta AI Hacked External Systems During Cybersecurity Testing	https://securityweek.com/meta-ai-hacked-external-systems-during-cybersecurity-testing
Meta AI Model Gained Internet Access and Hacked Another Organization's Network	https://cybersecuritynews.com/meta-ai-hacked-organizations

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
Claude Code and Gemini CLI Flaws Let a GitHub Issue Reach CI Workflow Secrets	https://thehackernews.com/2026/08/claude-code-and-gemini-cli-flaws-let.html
Multiple Flaws in Enterprise Java Platforms Allow Attackers to Execute Remote Code	https://cybersecuritynews.com/multiple-vulnerabilities-in-enterprise-java-platforms
New TONTOU CPU attack bypasses Spectre v2 fixes, leaks Linux password hashes	https://bleepingcomputer.com/news/security/new-tontou-cpu-attack-bypasses-spectre-v2-fixes-leaks-linux-password-hashes
New Zapscape KVM Flaw Could Let Privileged L1 Guest Code Escape to Linux Hosts	https://thehackernews.com/2026/08/new-zapscape-kvm-flaw-could-let.html
Public PoC Released for Linux Kernel Bridge Use-After-Free Vulnerability	https://cybersecuritynews.com/linux-kernel-bridge-use-after-free-vulnerability
Critical Jenkins Vulnerability Allows Attackers to Execute Malicious Code on Controller	https://cybersecuritynews.com/jenkins-code-execution-vulnerability
Critical Paperclip Flaw Allowed Admin Access, Code Execution	https://securityweek.com/critical-paperclip-flaw-allowed-admin-access-code-execution
Attackers Compile khunt Inside Oracle to Turn SQL Injection Into Windows SYSTEM Access	https://thehackernews.com/2026/08/attackers-compile-khunt-inside-oracle.html
AWS, Google, and Vercel Agent Flaws Let Attackers Trigger Tools Without Running the Model	https://thehackernews.com/2026/08/aws-google-and-vercel-patch-agent-flaws.html
CISA Flags TeamCity CVE-2026-63077 RCE Flaw Under Active Exploitation in the Wild	https://thehackernews.com/2026/08/cisa-flags-teamcity-cve-2026-63077-rce.html
Hackers Start Exploiting Recent JetBrains TeamCity Vulnerability	https://securityweek.com/hackers-start-exploiting-recent-jetbrains-teamcity-vulnerability

Apple iCloud Private Relay WebKit Flaws Leak Users' Real IP Addresses	https://cybersecuritynews.com/apple-icloud-private-relay
No Perfect Fix for AI Browser Prompt Injection Flaws	https://darkreading.com/application-security/no-perfect-fix-ai-browser-prompt-injection-flaws
How a $50,000 Exploit Chain Turned Bixby Against Samsung Phones	https://securityweek.com/how-a-50000-exploit-chain-turned-bixby-against-samsung-phones
Flaws in Google APK for Python Unlock Agent-to-Agent Attack	https://darkreading.com/vulnerabilities-threats/flaws-google-apk-python-agent-to-agent-attack
CISA warns of hackers exploiting Langflow, N-central, Apache Tomcat flaws	https://bleepingcomputer.com/news/security/cisa-warns-of-hackers-exploiting-langflow-n-central-apache-tomcat-flaws
Paperclip AI Flaws Let Attackers Run Host Commands via Malicious Agent Imports	https://thehackernews.com/2026/08/paperclip-ai-flaws-let-attackers-run.html
Paperclip AI Flaws Let Unauthenticated Attackers Run Commands	https://infosecurity-magazine.com/news/paperclip-ai-vulnerabilities-rce
Veeam, Terraform MCP, Django Patch Critical Flaws, Led by CVSS 10.0 Cross-Tenant Bug	https://thehackernews.com/2026/08/veeam-terraform-mcp-django-patch.html
New OVSwrap Linux Vulnerability Lets Attackers Gain Root Access	https://cybersecuritynews.com/ovswrap-linux-vulnerability

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
Critical Vulnerabilities Patched With Chrome 151 Update	https://securityweek.com/critical-vulnerabilities-patched-with-chrome-151-update
Anthropic Updates Claude Fable 5's Biology Safeguards to Reduce False Positives	https://cybersecuritynews.com/claude-fable-5s-biology-safeguards-update
Cisco Patches 12 SD-WAN and IOS XE Flaws, Including Three 9.9 CVSS Score Bugs	https://thehackernews.com/2026/08/cisco-patches-12-sd-wan-and-ios-xe.html
Cisco Patches Multiple Critical Cisco IOS XE Software Vulnerabilities - Patch Now!	https://cybersecuritynews.com/cisco-patches-ios-xe-software-vulnerabilities
Cisco Patches Critical SD-WAN, IOS XE, FMC Vulnerabilities	https://securityweek.com/cisco-patches-critical-sd-wan-ios-xe-fmc-vulnerabilities
Cisco Patched Multiple Critical Vulnerabilities in Catalyst SD-WAN - Update Now	https://cybersecuritynews.com/cisco-catalyst-sd-wan-vulnerabilities-2
TP-Link patches Omada ZTP flaws allowing hackers to breach networks	https://bleepingcomputer.com/news/security/tp-link-patches-omada-ztp-flaws-allowing-hackers-to-breach-networks

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
Malware Can Abuse Windows Hello for Business Keys for Persistent Entra ID Access	https://thehackernews.com/2026/08/malware-can-abuse-windows-hello-for.html
Ransomware Surges in July After Q2 Lull	https://infosecurity-magazine.com/news/ransomware-surges-july-q2-lull
Shai-Hulud CHAINDROP Worm Backdoors 400+ npm Packages With 1.3 Billion Monthly Downloads	https://cybersecuritynews.com/shai-hulud-chaindrop-worm-backdoors
TeamPCP Linked To Redis Attacks Dating Back To 2020 And Later Sup-ply Chain Campaign	https://thehackernews.com/2026/08/teampcp-linked-to-redis-attacks-dating.html
Zbtlink Chinese Router Sold Worldwide Contains a Hidden Backdoor Affecting 20+ Models	https://cybersecuritynews.com/zbtlink-chinese-router
ClickFix attack pushes macOS infostealer for crypto theft attacks	https://bleepingcomputer.com/news/security/clickfix-attack-pushes-macos-infostealer-for-crypto-theft-attacks
Hedge fund cyberattacks tied to BlackFile-linked UNC6671 extortion group	https://bleepingcomputer.com/news/security/hedge-fund-cyberattacks-tied-to-blackfile-linked-unc6671-extortion-group
SilverFox Hijacks Trusted Software and Kernel Drivers to Disable Secu-rity Tools	https://cybersecuritynews.com/silverfox-hijacks-trusted-software
Vanta Stealer Empties Browser Vaults, Crypto Wallets and Gaming Ac-counts in Minutes	https://cybersecuritynews.com/vanta-stealer-empties-browser-vaults
Hackers Can Leverage WSUS Servers to Deliver Malware and Compro-mise Enterprise Endpoints	https://cybersecuritynews.com/wsus-servers-leveraged-to-deliver-malware
ThreatsDay: Odysseus RCE, Samsung One-Click Takeover, iCloud Backdoor Fight + 27 More Stories	https://thehackernews.com/2026/08/threatsday-odysseus-rce-samsung-one.html
TeamPCP Traced Back to 2020 Cryptojacking Operation	https://infosecurity-magazine.com/news/teampcp-shadowray-ta-natalstatus
250+ macOS ClickFix Domains Use Browser Fingerprinting to Hide Atomic Stealer Attacks	https://cybersecuritynews.com/158536-2250-macos-clickfix-domains
New Shai-Hulud Supply Chain Attack Compromised 400+ Popular npm Packages	https://cybersecuritynews.com/new-npm-supply-chain-attack
COLDCARD security audit phishing attack installs remote access tool	https://bleepingcomputer.com/news/security/coldcard-security-audit-phishing-attack-installs-remote-access-tool
Hackers Turned Microsoft Logins, Zoom Events, and Government Web-sites Into Attack Tools	https://cybersecuritynews.com/hackers-turned-microsoft-logins-into-attack-tools
Google Blogger locks hundreds of blogs in malware false positive	https://bleepingcomputer.com/news/google/google-blogger-locks-hundreds-of-blogs-in-malware-false-positive
Three PhaaS Kits Targeting US Organizations to Steal M65 Logins by Bypassing MFA	https://cybersecuritynews.com/phaas-kits-targeting-us-organizations
New Attack Methods Enable Malware to Hijack Passkey-Protected Ac-counts	https://securityweek.com/new-attack-methods-enable-malware-to-hijack-passkey-protected-accounts
ChainDrop Worm Hits 400 npm Packages with Two Billion Monthly In-stalls	https://infosecurity-magazine.com/news/chaindrop-worm-400-npm-two-billion

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
Top 10 Best Protective DNS (PDNS) Services in 2026	https://cybersecuritynews.com/bst-protective-dns-services
Top 10 Best DNS Security Solutions in 2026	https://cybersecuritynews.com/best-dns-security-solutions
Top 10 Best Network Traffic Analysis (NTA) Tools in 2026	https://cybersecuritynews.com/best-network-traffic-analysis-tools
Top 10 Best Network Detection & Response (NDR) Tools in 2026	https://cybersecuritynews.com/best-ndr-solutions
Toolkit Hidden Inside Oracle Database Evades Endpoint Tools	https://infosecurity-magazine.com/news/khunt-toolkit-oracle-database-sql
OWASP Releases GenAI LLM Top 10 2026 for Building and Securing Modern AI Apps	https://cybersecuritynews.com/owasp-genai-llm-top-10-2026
Hackers run khunt post-exploitation toolkit from Oracle database	https://bleepingcomputer.com/news/security/hackers-run-khunt-post-exploitation-toolkit-from-oracle-database
Prompt Injection Remains Biggest LLM Risk, Despite Limited Incidents	https://infosecurity-magazine.com/news/prompt-injection-llm-risk

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 05/08/2026–07/08/2026 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/