

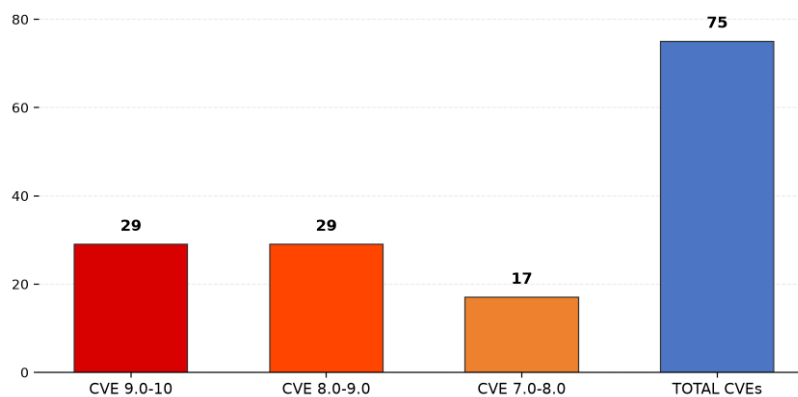


Newsletter on system vulnerabilities and cybersecurity news.

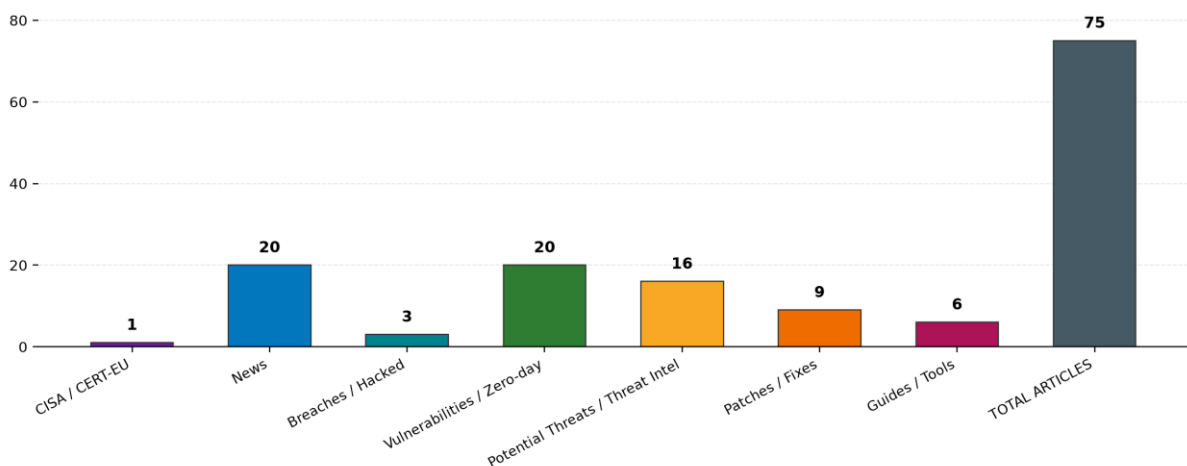
National Cyber Security Authority (NCSA)

Date: 09/09/2026 - 11/09/2026

of CVEs per CVSS score



of articles per section



Contents

Common Vulnerabilities and Exposures (CVEs)	3
CISA/CERT-EU Alerts & Advisories	9
News.....	9
Breaches / Compromised / Hacked.....	10
Vulnerabilities / Flaws / Zero-day.....	11
Patches / Updates / Fixes	12
Potential threats / Threat intelligence	12
Guides / Tools.....	13
References.....	14
Annex - Websites with vendor specific vulnerabilities	15

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-2026-89094	9,9	Forgejo	Improper Neutralization of Special Elements Used in a Template Engine	before 16.0.4	https://codeberg.org/forgejo/forgejo/milestone/139655 https://news.vcombinator.com/item?id=49645907			
CVE-2026-78573	9,8	IBM ContextForge MCP Gateway	Use of Default Credentials	1.0.0 through 1.0.7	https://www.ibm.com/support/pages/node/7286834			
CVE-2026-79724	9,8	IBM Langflow OSS	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	1.0.0 through 1.11.5	https://www.ibm.com/support/pages/node/7286666			
CVE-2026-87534	9,8	WebView in Google Chrome on Android	Missing Authorization	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html https://issues.chromium.org/issues/513134173	none	no	partial
CVE-2026-87544	9,8	Extensions in Google Chrome	Incorrect Authorization	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html			
CVE-2026-8778	9,8	MIPL Grouped Checkout Fields for WooCommerce. Customize & Organize Checkout Fields.	Unrestricted Upload of File with Dangerous Type	up to, and including, 1.2.1.	https://plugins.trac.wordpress.org/browser/mipl-wc-checkout-fields/tags/1.2.1/include/class-mipl-wc-cf-checkout-block.php#L415 https://plugins.trac.wordpress.org/browser/mipl-wc-checkout-fields/tags/1.2.1/mipl-wc-checkout-fields.php#L260 https://plugins.trac.wordpress.org/browser/mipl-wc-checkout-fields/trunk/include/class-mipl-wc-cf-checkout-block.php#L415 https://plugins.trac.wordpress.org/browser/mipl-wc-checkout-fields/trunk/mipl-wc-checkout-fields.php#L260 https://plugins.trac.wordpress.org/changeset?sfp_email=&sfp_mail=&reponame=&new=3552029%40mipl-wc-checkout-fields%2Ftrunk%2Finclude%2Fclass-mipl-wc-cf-checkout-block.php&old=3549283%40mipl-wc-checkout-fields%2Ftrunk%2Finclude%2Fclass-mipl-wc-cf-checkout-block.php&sfp_email=&sfp_mail= https://www.wordfence.com/threat-intel/vulnerabilities/id/ac1257a9-7c8e-43aa-b21a-93a77b456aa4?source=cve			
CVE-2026-82100	9,6	IBM DataStage on Cloud Pak for Data	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	5.4.0.0	https://www.ibm.com/support/pages/node/7286562			
CVE-2026-87438	9,6	WebGL in Google Chrome on Android	Out-of-bounds Write	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87448	9,6	DevTools in Google Chrome	Use After Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87455	9,6	Aura in Google Chrome	Use After Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	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-2026-87464	9,6	WebGL in Google Chrome	Use After Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87470	9,6	Tint in Google Chrome on on Mac	Improper Validation of Specified Quantity in Input	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87474	9,6	Payments in Google Chrome	Use After Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87494	9,6	Browser in Google Chrome on on Windows	Use After Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87500	9,6	ANGLE in Google Chrome	Improper Validation of Array Index	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87504	9,6	Core in Google Chrome	Use After Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87512	9,6	ANGLE in Google Chrome on on Windows	Use After Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87520	9,6	Dawn in Google Chrome on on Android	Use After Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87526	9,6	Passwords in Google Chrome	Use After Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87528	9,6	Rust in Google Chrome on on Windows	Access of Resource Using Incompatible Type ('Type Confusion')	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html https://issues.chromium.org/issues/539569491	none	no	total
CVE-2026-87529	9,6	Media in Google Chrome	Numeric Truncation Error	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87547	9,6	FileSystem in Google Chrome	Use of Incorrectly-Resolved Name or Reference	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87558	9,6	Payments in Google Chrome on on Mac	Use After Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87607	9,6	Device in Google Chrome on on Mac	Use After Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87609	9,6	Sharing in Google Chrome on on iOS	Use After Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87634	9,6	WebPackaging in Google Chrome	Use After Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87637	9,6	Extensions in Google Chrome on on Mac	Use After Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87643	9,6	GPU in Google Chrome on on Android	Integer Overflow or Wraparound	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87646	9,6	Web Authentication in Google Chrome	Use After Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-73784	8,8	HPE IceWall products	Improper Verification of Cryptographic Signature	4.0	https://support.hpe.com/hpsc/public/docDisplay?docId=hpesbmu05142en_us&docLocale=en_US			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-80914	8,8	Linux		ccf74f2390d60a2f9a75e f496d2564abb478f46a prior to 2387cd06a2c0b416f050 28b02bba1089f54c28d9; ccf74f2390d60a2f9a75e f496d2564abb478f46a prior to 49fd7116f76b860b2308 43700fb7423ab5331e1f ; ccf74f2390d60a2f9a75e f496d2564abb478f46a prior to 03288b7447c9e572f8a b82fc29cfb4ca719ab210; ccf74f2390d60a2f9a75e f496d2564abb478f46a prior to 560bef609fa599274592 9e8d7d458b9d88dd2830; 6.0	https://git.kernel.org/stable/c/03288b7447c9e572f8ab82fc29cfb4ca719ab210 https://git.kernel.org/stable/c/2387cd06a2c0b416f05028b02bba1089f54c28d9 https://git.kernel.org/stable/c/49fd7116f76b860b230843700fb7423ab5331e1f https://git.kernel.org/stable/c/560bef609fa5992745929e8d7d458b9d88dd2830			
CVE-2026-81996	8,8	Acrobat Reader	Incorrect Authorization	versions from (including) 24.0.0 up to (excluding) 24.001.30429; versions from (including) 15.008.20082 up to (excluding) 26.002.21901	https://helpx.adobe.com/security/products/acrobat/apsb26-141.html	none	no	total
CVE-2026-87430	8,8	WebRTC in Google Chrome	Heap-based Buffer Overflow	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87433	8,8	FileAPI in Google Chrome	Time-of-check Time-of-use (TOCTOU) Race Condition	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87444	8,8	Codecs in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87460	8,8	Platform in Google Chrome	Use After Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87489	8,8	V8 in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87542	8,8	Input in Google Chrome	Use After Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87569	8,8	Views in Google Chrome	Missing Authorization	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87570	8,8	SiteIsolation in Google Chrome	Incorrect Authorization	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87585	8,8	PDFium in Google Chrome on on Windows	Double Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87588	8,8	Chromecast in Google Chrome	Use After Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	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-2026-87636	8,8	XML in Google Chrome	Access of Resource Using Incompatible Type ('Type Confusion')	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87480	8,3	Printing in Google Chrome	Use After Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87506	8,3	WebUI in Google Chrome	Execution with Unnecessary Privileges	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87524	8,3	Core in Google Chrome on on Windows	Use After Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87578	8,3	Receiver in Google Chrome	Use After Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87582	8,3	DataTransfer in Google Chrome	Unintended Proxy or Intermediary ('Confused Deputy')	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87616	8,3	Views in Google Chrome on on Windows	Improper Initialization	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87618	8,3	Storage in Google Chrome on on Windows	Use of Incorrectly-Resolved Name or Reference	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87628	8,3	Cast in Google Chrome	Use After Free	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-19991	8,1	The UsersWP plugin for Word-Press	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	up to, and including, 1.2.70	https://plugins.trac.wordpress.org/browser/userswp/tags/1.2.70/includes/class-forms.php#L2076 https://plugins.trac.wordpress.org/browser/userswp/tags/1.2.70/includes/class-forms.php#L2420 https://plugins.trac.wordpress.org/browser/userswp/tags/1.2.70/includes/class-forms.php#L2432 https://plugins.trac.wordpress.org/browser/userswp/tags/1.2.70/includes/class-validation.php#L194 https://plugins.trac.wordpress.org/browser/userswp/tags/1.2.70/includes/helpers/misc.php#L2107 https://plugins.trac.wordpress.org/changeset?sfnp_email=&sfph_mail=&reponame=&new=3650759%40userswp%2Ftrunk&old=3618724%40userswp%2Ftrunk&sfnp_email=&sfph_mail=			
CVE-2026-65181	8,1	Impala	Improper Control of Dynamically-Managed Code Resources	versions from (including) 2.7.0 up to (excluding) 4.5.2	https://lists.apache.org/thread/2tv3srsh96i86xxq4q1hb05rwszwcml http://www.openwall.com/lists/oss-security/2026/09/08/24	none	no	total
CVE-2026-87457	8,1	Updater in Google Chrome on on Windows	Time-of-check Time-of-use (TOCTOU) Race Condition	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87471	8,1	ServiceWorker in Google Chrome	Incorrect Authorization	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87499	8,1	Network in Google Chrome	Incorrect Authorization	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87530	8,1	CredentialProvider in Google Chrome on on Windows	Uncontrolled Search Path Element	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	no	total
CVE-2026-87554	8,1	Chromoting in Google Chrome on on Windows	Time-of-check Time-of-use (TOCTOU) Race Condition	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	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-2026-21087	7,8	libmdnie	Out-of-bounds Write	15.0; 16.0; 17.0	https://security.samsungmobile.com/securityUpdate.smsb?year=2026&month=09	none	no	total
CVE-2026-21088	7,8	loading a subtitle frame in libsubextractor	Improper Input Validation	14.0; 15.0; 16.0; 17.0	https://security.samsungmobile.com/securityUpdate.smsb?year=2026&month=09	none	no	partial
CVE-2026-21089	7,8	removing style tag in libsubextractor	Improper Input Validation	14.0; 15.0; 16.0; 17.0	https://security.samsungmobile.com/securityUpdate.smsb?year=2026&month=09	none	no	partial
CVE-2026-2310	7,8	IBM webMethods Integration Server	XML Injection (aka Blind XPath Injection)	11.1	https://www.ibm.com/support/pages/node/7286620			
CVE-2026-81210	7,7	DataStage on Cloud Pak for Data	Authorization Bypass Through User-Controlled Key	5.4.0.0	https://www.ibm.com/support/pages/node/7286562			
CVE-2026-89060	7,7	multicloud-observability-addon	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization		https://access.redhat.com/security/cve/CVE-2026-89060 https://bugzilla.redhat.com/show_bug.cgi?id=2531596 https://github.com/stolostron/multicloud-observability-addon/pull/644			
CVE-2026-15462	7,5	The Sticky Chat Widget plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to, and including, 1.4.2.	https://plugins.trac.wordpress.org/browser/sticky-chat-widget/tags/1.4.2/includes/front-end.php#L141 https://plugins.trac.wordpress.org/browser/sticky-chat-widget/tags/1.4.2/includes/front-end.php#L188 https://plugins.trac.wordpress.org/browser/sticky-chat-widget/tags/1.4.2/includes/front-end.php#L60 https://plugins.trac.wordpress.org/changeset?sfnp_email=&sfph_mail=&reponame=&new=3640407%40sticky-chat-widget%2Ftrunk%2Fincludes%2Ffront-end.php&old=3349742%40sticky-chat-widget%2Ftrunk%2Fincludes%2Ffront-end.php&sfph_email=&sfph_mail= https://www.wordfence.com/threat-intel/vulnerabilities/id/35a49ba9-02a6-47cf-98f0-053b06036b08?source=cve			
CVE-2026-18561	7,5	The Unlimited Elements For Elementor plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to, and including, 2.0.16.	https://plugins.trac.wordpress.org/browser/unlimited-elements-for-elementor/trunk/inc_php/framework/db.class.php#L216 https://plugins.trac.wordpress.org/browser/unlimited-elements-for-elementor/trunk/inc_php/unitecreator_actions.class.php#L87 https://plugins.trac.wordpress.org/browser/unlimited-elements-for-elementor/trunk/inc_php/unitecreator_addon.class.php#L304 https://plugins.trac.wordpress.org/browser/unlimited-elements-for-elementor/trunk/inc_php/unitecreator_addons.class.php#L1387 https://plugins.trac.wordpress.org/browser/unlimited-elements-for-elementor/trunk/provider/provider_functions.class.php#L611 https://plugins.trac.wordpress.org/changeset?sfnp_email=&sfph_mail=&reponame=&new=3661670%40unlimited-elements-for-elementor%2Ftrunk&old=3628543%40unlimited-elements-for-elementor%2Ftrunk&sfph_email=&sfph_mail=			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-73785	7,5	HPE IceWall Federation Agent and Proxy	Improper Handling of Unexpected Data Type	4.0	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbmu05147en_us&docLocale=en_US			
CVE-2026-77807	7,5	The AcyMailing – An Ultimate Newsletter Plugin and Marketing Automation Solution for WordPress plugin for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	up to, and including, 11.0.4	https://plugins.trac.wordpress.org/changeset/3679457/ https://www.wordfence.com/threat-intel/vulnerabilities/id/19a9b952-84db-4911-bb50-52d74ec01cb8?source=cve			
CVE-2026-78130	7,5	strongSwan	NULL Pointer Dereference	4.2.0 through 6.0.7	https://github.com/strongswan/strongswan/releases/tag/6.1.0 https://www.strongswan.org/blog/2026/09/07/strongswan-vulnerability-(cve-2026-78130).html			
CVE-2026-87450	7,5	Permissions in Google Chrome	Incorrect Authorization	prior to 153.0.8010.36	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html	none	yes	partial
CVE-2026-87908	7,5	multiparty	Uncontrolled Resource Consumption; Allocation of Resources Without Limits or Throttling	4.3.1 or later	https://cna.openisf.org/security-advisories.html https://github.com/billaris/multiparty/security/advisories/GHSA-5h46-2939-q3wh			
CVE-2026-89161	7,4	In PCRE2	Free of Memory not on the Heap	before 10.48	https://github.com/PCRE2Project/pcre2/pull/937 https://github.com/PCRE2Project/pcre2/releases/tag/pcre2-10.48			
CVE-2026-18579	7,2	The WP Photo Album Plus plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 9.2.08.003	https://plugins.trac.wordpress.org/browser/wp-photo-album-plus/tags/9.2.07.002/wppa-admin-scripts.js#L2069 https://plugins.trac.wordpress.org/browser/wp-photo-album-plus/tags/9.2.07.002/wppa-ajax.php#L1246 https://plugins.trac.wordpress.org/browser/wp-photo-album-plus/tags/9.2.07.002/wppa-input.php#L560 https://plugins.trac.wordpress.org/browser/wp-photo-album-plus/tags/9.2.07.002/wppa-utils.php#L1960 https://plugins.trac.wordpress.org/browser/wp-photo-album-plus/tags/9.2.08.003/js/wppa-admin-scripts.js#L2069 https://plugins.trac.wordpress.org/browser/wp-photo-album-plus/tags/9.2.08.003/wppa-ajax.php#L1246			
CVE-2026-81754	7,2	The Vigilant –	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 2.10.2	https://plugins.trac.wordpress.org/browser/vigilante/tag/s/2.9.5/assets/js/admin.js#L1996 https://plugins.trac.wordpress.org/browser/vigilante/tag/s/2.9.5/assets/js/admin.js#L2778 https://plugins.trac.wordpress.org/browser/vigilante/tag/s/2.9.5/includes/class-database.php#L448 https://plugins.trac.wordpress.org/browser/vigilante/tag/s/2.9.5/includes/class-database.php#L639 https://plugins.trac.wordpress.org/browser/vigilante/tag/s/2.9.5/includes/class-login-security.php#L899 https://plugins.trac.wordpress.org/changeset?sfp_email=&sfp_mail=&reponame=&new=3669625%40vigilante%2Ftrunk%2Fassets%2Fjs%2Fadmin.js&old=3667821%40vigilante%2Ftrunk%2Fassets%2Fjs%2Fadmin.js&sfp_email=&sfp_mail=			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-81825	7,2	The Simple Ajax Chat – Add a Fast, Secure Chat Box plugin for Word-Press	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20260811 and earlier	https://plugins.trac.wordpress.org/browser/simple-ajax-chat/trunk/simple-ajax-chat-core.php#L34 https://plugins.trac.wordpress.org/browser/simple-ajax-chat/trunk/simple-ajax-chat-form.php#L143 https://plugins.trac.wordpress.org/browser/simple-ajax-chat/trunk/simple-ajax-chat-form.php#L144 https://plugins.trac.wordpress.org/browser/simple-ajax-chat/trunk/simple-ajax-chat-form.php#L182 https://plugins.trac.wordpress.org/browser/simple-ajax-chat/trunk/simple-ajax-chat.php#L329 https://plugins.trac.wordpress.org/browser/simple-ajax-chat/trunk/simple-ajax-chat.php#L698			

CISA/CERT-EU Alerts & Advisories

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

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds Two Known Exploited Vulnerabilities to Catalog CISA	CVE-2026-67277 MikroTik RouterOS Missing Authentication for Critical Function Vulnerability CVE-2026-86060 MikroTik RouterOS Improper Neutralization of Argument Delimiters in a Command Vulnerability	https://cisa.gov/news-events/alerts/2026/09/10/cisa-adds-two-known-exploited-vulnerabilities-catalog

News

Η ενότητα "News" συνοψίζει τα πιο σημαντικά γεγονότα της εβδομάδας στον τομέα της κυβερνοασφάλειας. Εδώ θα βρείτε επιθέσεις που ξεχώρισαν, νέες τεχνικές που εντοπίστηκαν, ή ενέργειες από γνωστές ομάδες hacking. Δίνει την απαραίτητη εικόνα του τι συμβαίνει διεθνώς και πού πρέπει να στραφεί η προσοχή.

Σύντομη περιγραφή / Τίτλος	URL
Microsoft Investigating Microsoft 365 Copilot Access Issues Under Incident CP1470554	https://cybersecuritynews.com/microsoft-365-copilot-access-issues
Conti ransomware gang member sentenced to 4 years in prison	https://bleepingcomputer.com/news/security/conti-ransomware-gang-member-sentenced-to-four-years-in-prison
Remote Desktop Services Failures on Windows Servers Following September Update	https://cybersecuritynews.com/remote-desktop-services-failures
September Windows Server updates break Remote Desktop Services	https://bleepingcomputer.com/news/microsoft/september-windows-server-updates-break-remote-desktop-services
Mandiant Founder Kevin Mandia Joins Amazon Board	https://securityweek.com/mandiant-founder-kevin-mandia-joins-amazon-board

Surfshark VPN says hackers breached internal testing, proxy servers	https://bleepingcomputer.com/news/security/surfshark-vpn-says-hackers-breached-internal-testing-proxy-servers
Microsoft Excel KB5002914 update breaks copy and paste for some users	https://bleepingcomputer.com/news/microsoft/microsoft-excel-kb5002914-update-breaks-copy-and-paste-for-some-users
Cybersecurity M&A Roundup: 33 Deals Announced in August 2026	https://securityweek.com/cybersecurity-ma-roundup-33-deals-announced-in-august-2026
Nightmare-Eclipse Strikes Again With ShieldCrash Windows Exploit	https://darkreading.com/vulnerabilities-threats/nightmare-eclipse-strikes-again-shieldcrash-windows-exploit
Anthropic Researcher Resigns With Warning About the Dangers of AI Development	https://securityweek.com/anthropic-researcher-resigns-with-warning-about-the-dangers-of-ai-development
Hacker Conversations: Vinnie Liu, Performer Turned Ringmaster	https://securityweek.com/hacker-conversations-vinnie-liu-performer-turned-ringmaster
WordPress Uses AI to Stop Malicious Plugin Updates Before They Reach Millions of Websites	https://cybersecuritynews.com/wordpress-uses-ai-to-stop-malicious-plugin
Deceptive Android Apps Exploit Google Play Early Access to Evade Reviews	https://securityweek.com/deceptive-android-apps-exploit-google-play-early-access-to-evade-reviews
Webinar Today: Keep Pace With AI - A New Operating Model for Endpoint Remediation	https://securityweek.com/webinar-today-keep-pace-with-ai-a-new-operating-model-for-endpoint-remediation
FBI Publishes First-Ever Cyber Strategy, With Focus on Disrupting Threats	https://infosecurity-magazine.com/news/fbi-cyber-strategy-disrupting
Widened Scan Turns Up Fourth Rogue Claude Cyber Incident	https://securityweek.com/widened-scan-turns-up-fourth-rogue-claude-cyber-incident
PaperCut Attacker Uses Hundreds of AI Agents to Compromise 440+ Instances	https://thehackernews.com/2026/09/papercut-attacker-uses-hundreds-of-ai.html
Microsoft says September updates fix mouse settings reset issues	https://bleepingcomputer.com/news/microsoft/microsoft-resolves-mouse-settings-reset-bug-windows-11-update
Anthropic Reveals Yet Another Cybersecurity Incident	https://infosecurity-magazine.com/news/anthropic-another-cybersecurity
Privacy Policy	https://cybersecuritynews.com/privacy-policy-2

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
IDScan confirms breach tied to 153 million stolen driver's licenses	https://bleepingcomputer.com/news/security/idscan-confirms-breach-tied-to-153-million-stolen-drivers-licenses
4.1 Million Impacted by AdaptHealth Data Breach	https://securityweek.com/4-1-million-impacted-by-adapthealth-data-breach
Veradigm Confirms Patient Data Exposed in Third-Party Data Breach	https://cybersecuritynews.com/veradigm-patient-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
Attackers Chain JFrog Artifactory Flaws to Gain Admin Control and Plant Backdoors	https://thehackernews.com/2026/09/attackers-chain-jfrog-artifactory-flaws.html
Skullcandy Dime 3 Bluetooth Flaw Lets Nearby Attackers Hijack Audio and Spy Through Microphone	https://cybersecuritynews.com/skullcandy-dime-3-bluetooth-flaw
AI-powered attack exploited PaperCut flaws to hack 395 organizations	https://bleepingcomputer.com/news/security/ai-powered-attack-exploited-papercut-flaws-to-hack-395-organizations
New 'BlueMoon' kit exploited Windows and Chrome zero-day flaws	https://bleepingcomputer.com/news/security/new-bluemoon-kit-exploited-windows-and-chrome-zero-day-flaws
Critical Check Point VPN Vulnerabilities Enable Remote Code Execution Attacks	https://cybersecuritynews.com/check-point-vpn-vulnerabilities
Critical NetScaler Vulnerability Exploited in Attacks	https://securityweek.com/critical-netscaler-vulnerability-exploited-in-attacks
Check Point Discloses Two 9.8-Rated VPN Certificate Flaws Enabling Unauthenticated RCE	https://thehackernews.com/2026/09/check-point-discloses-two-98-rated-vpn.html
Palo Alto PAN-OS Vulnerability Enables Arbitrary Code Execution as Root User	https://cybersecuritynews.com/palo-alto-pan-os-vulnerability-code-execution
CISA Flags Exploited Cisco, Citrix, Fortinet Flaws, Sets Sept. 12 Federal Patch Deadline	https://thehackernews.com/2026/09/cisa-flags-exploited-cisco-citrix.html
Organizations Warned of Cisco Secure FMC Exploitation	https://securityweek.com/organizations-warned-of-cisco-secure-fmc-exploitation
New 'ShieldCrash' Zero-Day Exploit Targets Microsoft Defender	https://securityweek.com/new-shieldcrash-zero-day-exploit-targets-microsoft-defender
Fortinet Code Execution Flaw Exploited in PivotC2 RAT Attacks	https://securityweek.com/fortinet-code-execution-flaw-exploited-in-pivotc2-rat-attacks
Cisco confirms CVE-2026-20079 Secure FMC flaw exploited in attacks	https://bleepingcomputer.com/news/security/cisco-confirms-cve-2026-20079-secure-fmc-flaw-exploited-in-attacks
Mythos Vulnerability Firehose Hits a Human Bottleneck	https://darkreading.com/application-security/mythos-vulnerability-firehose-hits-human-bottleneck
Android's September 2026 Updates Patch 180 Vulnerabilities	https://securityweek.com/androids-september-2026-updates-patch-180-vulnerabilities
Hackers Use Hundreds of AI Agents to Exploit PaperCut Flaws and Compromise 440 Servers Worldwide	https://cybersecuritynews.com/papercut-flaws-compromised-using-ai
DeepSeek Harness Flaw Let AI Agents Disable Their Own File Sandbox Without Approval	https://thehackernews.com/2026/09/deepseek-harness-flaw-let-ai-agents.html
ICS Patch Tuesday: Schneider Electric, Siemens Fix Critical Flaws	https://securityweek.com/ics-patch-tuesday-schneider-electric-siemens-fix-critical-flaws
Alby Hub Critical Flaw Could Let Attackers Take Over Internet-Exposed Bitcoin Wallets	https://thehackernews.com/2026/09/alby-hub-critical-flaw-could-let.html
Over 36,000 exposed Plex servers vulnerable to recent flaws	https://bleepingcomputer.com/news/security/over-36-000-plex-servers-unpatched-against-recently-disclosed-flaws

Patches / Updates / Fixes

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

Σύντομη περιγραφή / Τίτλος	URL
PaperCut Replaces Emergency Patches With Fixes for Two Actively Exploited Flaws	https://thehackernews.com/2026/09/papercut-replaces-emergency-patches.html
CISA Updates Insider Threat Guide With New Mitigation Advice	https://infosecurity-magazine.com/news/cisa-updates-insider-threat-guide
Microsoft fixes bug that wiped Windows desktop settings	https://bleepingcomputer.com/news/microsoft/microsoft-fixes-bug-that-wiped-windows-desktop-settings
Fortinet Patches Critical Vulnerabilities in FortiMonitorOnSight, Chrome Extension	https://securityweek.com/fortinet-patches-critical-vulnerabilities-in-fortimonitoronsight-chrome-extension
Ivanti Patches Critical Flaws Across Enterprise Security Products	https://securityweek.com/ivanti-patches-critical-flaws-across-enterprise-security-products
Chrome 153 Patches Seventh Zero-Day of 2026	https://securityweek.com/chrome-153-patches-seventh-zero-day-of-2026
SAP Patches Maximum Severity “Overpass” Flaw	https://infosecurity-magazine.com/news/sap-patches-maximum-severity
SAP Patches CVSS 10.0 Kernel Flaw Enabling Unauthenticated Remote Code Execution	https://thehackernews.com/2026/09/sap-patches-cvss-100-kernel-flaw.html
Microsoft Patches Record 974 Flaws, Including Two Exploited Windows Zero-Days	https://thehackernews.com/2026/09/microsoft-patches-record-974-flaws.html

Potential threats / Threat intelligence

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

Σύντομη περιγραφή / Τίτλος	URL
Harley-Davidson Alleged Breach - CL0P Ransomware Adds Motorcycle Maker to the List	https://cybersecuritynews.com/harley-davidson-alleged-breach
China-Linked UNC3569 Exploited Sogou Input Method Flaw to Deploy GRAYRABBIT Backdoor	https://thehackernews.com/2026/09/china-linked-unc3569-exploited-sogou.html
Cisco FMC Flaws Exploited to Steal Credentials and Deploy Qilin Ransomware	https://thehackernews.com/2026/09/cisco-fmc-flaws-exploited-to-steal.html
Hackers Use Claude AI Agents to Automate Cyberattacks, Develop 0-Days and Evade Detection	https://cybersecuritynews.com/claude-ai-agents-used-to-automate-cyberattacks
New Android malware encrypts files, steals data, and harasses victims	https://bleepingcomputer.com/news/security/new-android-malware-encrypts-files-steals-data-and-harasses-victims
ThreatsDay: 200 Android Flaws, Browser-Built Phishing, 119K Scam Shops + 23 More Stories	https://thehackernews.com/2026/09/threatsday-200-android-flaws-browser.html

Cisco FMC flaws exploited by ransomware gang, state-sponsored hackers	https://bleepingcomputer.com/news/security/cisco-fmc-flaws-exploited-by-ransomware-gang-state-sponsored-hackers
Hackers Use Fake GTA 6 Downloads to Deploy RATs, Infostealers and Data-Wiping Malware	https://cybersecuritynews.com/fake-gta-6-downloads
Hackers Exploit Critical Cisco Firewall Flaw to Gain Root Access and Deploy Malware	https://cybersecuritynews.com/cisco-firewall-root-access-flaw
Hackers Use Passkey-Themed Phishing to Hijack Microsoft 365 Accounts and Steal Cloud Data	https://cybersecuritynews.com/passkey-themed-phishing
MantaxOtax Android Malware Combines Ransomware With Spyware	https://infosecurity-magazine.com/news/mantaxotax-android-malware
CISA: WatchGuard RCE flaw now exploited in ransomware attacks	https://bleepingcomputer.com/news/security/cisa-watchguard-rce-flaw-now-exploited-in-ransomware-attacks
Trezor warns users of email provider breach, phishing attacks	https://bleepingcomputer.com/news/security/trezor-warns-users-of-email-provider-breach-phishing-attacks
Four Spy Groups Used the Same Chrome and Windows Exploit Kit Within a Week	https://thehackernews.com/2026/09/four-spy-groups-used-same-chrome-and.html
Researchers Build WeChat Zero-Click Worm Hijacking Phones via Calls	https://infosecurity-magazine.com/news/wechat-zeroclick-worm-hijack
F5 BIG-IP APM Malware Injects a PHP Web Shell Into Memory, Evading Disk Scans	https://thehackernews.com/2026/09/f5-big-ip-apm-malware-injects-php-web.html

Guides / Tools

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

Σύντομη περιγραφή / Τίτλος	URL
Top 10 Best CNAPP (Cloud-Native Application Protection) Platforms in 2026	https://cybersecuritynews.com/best-cnapp-platforms
Top 10 Best Cloud Workload Protection (CWPP) Solutions in 2026	https://cybersecuritynews.com/best-cwpp-solutions
Top 10 Best Cloud Security Posture Management (CSPM) Tools in 2026	https://cybersecuritynews.com/best-cspm-tools
Top 10 Best Enterprise Browsers in 2026	https://cybersecuritynews.com/best-enterprise-browsers
Top 10 Best Browser Isolation Solutions in 2026	https://cybersecuritynews.com/best-browser-isolation-solutions
Webinar: Learn How to Answer “Are We Exposed?” Faster After a New CVE	https://thehackernews.com/2026/09/webinar-learn-how-to-answer-are-we.html

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 09/09/2026–11/09/2026, και έχει γίνει μια επιλογή συστημάτων/υπηρεσιών ανάλογα με το πόσο διαδεδομένα είναι.

Annex – Websites with vendor specific vulnerabilities

Ο πίνακας περιέχει websites από κατασκευαστές που προσφέρουν πληροφορίες σχετικές με ευπάθειες που εμφανίζονται στα προϊόντα τους.

Vendor name / Platform	URL
Wordpress	Wordfence Intelligence Vulnerability Database API https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/ Scan your WordPress website, https://wpscan.com/scan/
Oracle	Critical Patch Updates, Security Alerts and Bulletins, https://www.oracle.com/security-alerts/
Fortinet	Fortinet products, https://www.fortiguard.com/psirt
IBM	Security bulletins, https://cloud.ibm.com/status/security Research, Collaborate and Act on threat intelligence, https://exchange.xforce.ibmcloud.com/
MS Windows	The Microsoft Security Response Center (MSRC), https://msrc.microsoft.com/update-guide/
SAP	SAP Security Notes, https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html
Dell	Security Advisories, Notices and Resources, https://www.dell.com/support/security/en-us
HPE	HPE Security Bulletin Library, https://support.hpe.com/connect/s/securitybulletinlibrary Security Bulletins, https://support.hp.com/us-en/security-bulletins
Cisco	Cisco Security Advisories, https://sec.cloudapps.cisco.com/security/center/publicationListing.x
Palo Alto	Palo Alto Networks Security Advisories, https://security.paloaltonetworks.com/
Ivanti	Security Advisory, https://www.ivanti.com/blog/topics/security-advisory
Mozilla	Mozilla Foundation Security Advisories, https://www.mozilla.org/en-US/security/advisories/
Android	Android Security Bulletins, https://source.android.com/docs/security/bulletin/asb-overview
Zyxel	Security Advisories, https://www.zyxel.com/global/en/support/security-advisories
D-Link	Global Security Advisories, Responses, and Notices, https://supportannouncement.us.dlink.com/
Adobe	Security Bulletins and Advisories, https://helpx.adobe.com/security/security-bulletin.html
Siemens	Siemens ProductCERT and Siemens CERT, https://www.siemens.com/global/en/products/services/cert.html
Splunk	Splunk Security Advisories, https://advisory.splunk.com/