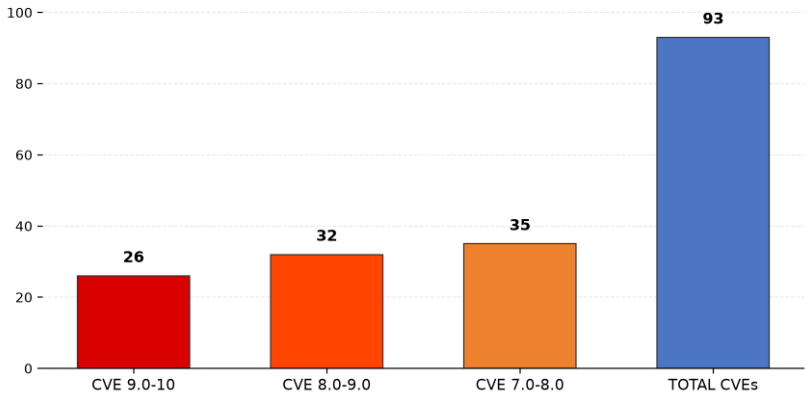
Newsletter on system vulnerabilities and cybersecurity news.

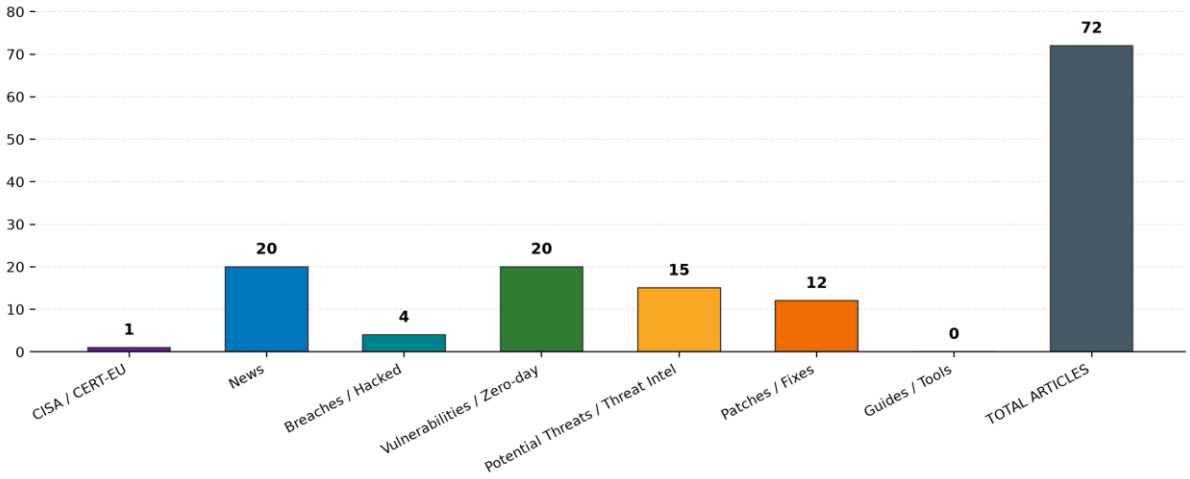
National Cyber Security Authority (NCSA)

Date: 14/10/2026 - 16/10/2026

# of CVEs per CVSS score



# of articles per section



Contents

Common Vulnerabilities and Exposures (CVEs) 3
CISA/CERT-EU Alerts & Advisories 18
News 18
Breaches / Compromised / Hacked 19
Vulnerabilities / Flaws / Zero-day 20
Patches / Updates / Fixes 21
Potential threats / Threat intelligence 22
Guides / Tools 22
References 23
Annex – Websites with vendor specific vulnerabilities 24

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-2026-106622	10,0	ColdFusion	Server-Side Request Forgery (SSRF)	2023; 2025	https://www.adobe.com/trust/security/products/coldfusion/apsb26-144.html	none	yes	total
CVE-2026-77524	9,9	KEDA	Improper Privilege Management; Server-Side Request Forgery (SSRF)	In version 2.20.2 and earlier	https://github.com/kedacore/keda/commit/1e21cc798dedd079e696cdb45388eddc5e18365d https://github.com/kedacore/keda/releases/tag/v2.21.0 https://github.com/kedacore/keda/security/advisories/GHSA-637c-6jxx-4rwm			
CVE-2026-97381	9,9	Legacy Update	Origin Validation Error; Return of Wrong Status Code	1.12.0 through 1.13.1	https://github.com/LegacyUpdate/LegacyUpdate/commit/7d62f0bfaa770d74cd6e2cb0bac9c1907df48033 https://github.com/LegacyUpdate/LegacyUpdate/commit/ae1c46c97f39a55a1937784d9f9beb30aa9147fd https://github.com/LegacyUpdate/LegacyUpdate/releases/tag/v1.13.2.0 https://github.com/LegacyUpdate/LegacyUpdate/security/advisories/GHSA-f4g7-4gmx-jfqf https://legacyupdate.net/news/2026/07/21/legacy-update-1-13-2			
CVE-2020-37282	9,8	office-converter	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	through 1.0.2	https://github.com/advisories/GHSA-9p64-h5g4-phpm https://github.com/vworld4u/office-converter/blob/b1ea855d0001dc7a5d66343698634dbc06b72c2d/index.js#L19-L20 https://github.com/vworld4u/office-converter/pull/9 https://www.vulncheck.com/advisories/office-converter-through-1.0.2-os-command-injection-via-filename-in-generatepdf			
CVE-2026-104798	9,8	The My Calendar – Accessible Event Manager plugin for WordPress	Improper Privilege Management	up to, and including, 3.8.7.	https://plugins.trac.wordpress.org/browser/my-calendar/tags/3.8.6/my-calendar-navigation.php#L248 https://plugins.trac.wordpress.org/browser/my-calendar/tags/3.8.6/my-calendar-navigation.php#L260 https://plugins.trac.wordpress.org/browser/my-calendar/tags/3.8.6/my-calendar-output.php#L1622 https://plugins.trac.wordpress.org/browser/my-calendar/tags/3.8.6/my-calendar-search.php#L170 https://plugins.trac.wordpress.org/browser/my-calendar/tags/3.8.6/my-calendar-search.php#L221 https://plugins.trac.wordpress.org/browser/my-calendar/tags/3.8.6/my-calendar-shortcodes.php#L102			
CVE-2026-108065	9,8	the SOAP GetUser method of the /pre-approval	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.* and earlier	https://www.rapid7.com/blog/post/ve-unauthenticated-sql-injection-in-channel-software-weballiance-ecommerce/	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-2026-110612	9,8	vlife	Use of Hard-coded Cryptographic Key	through 2.0.1	https://github.com/wwwlike/vlife https://github.com/wwwlike/vlife/blob/4f03b19b91d82781939653f5b0d9a70721734d6d/vlife-base/src/main/java/cn/wwwlike/config/VlifeUrlDecisionManager.java#L25 https://github.com/wwwlike/vlife/blob/4f03b19b91d82781939653f5b0d9a70721734d6d/vlife-boot-starter-web/src/main/java/cn/wwwlike/web/security/filter/TokenUtil.java#L33-L58 https://hackmd.io/@1ExmmukzRMWN7B4qO4W-4Q/vlife-hardcoded-jwt-secret-token-forgery https://www.vulncheck.com/advisories/vlife-through-2.0.1-authentication-bypass-via-hardcoded-jwt-secret-in-tokenutil	poc	yes	total
CVE-2026-110634	9,8	git-diff	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	before 2.0.7	https://github.com/danday74/git-diff https://github.com/danday74/git-diff/blob/a85a649badc4c6bba991e87e82382b7d3cdd6634/js/gitDiffReal/generateDiff/index.js#L26-L30 https://github.com/danday74/git-diff/commit/bfd727b6cf1daa671c3528d1d681f55b70e8fb19 https://github.com/danday74/git-diff/pull/16 https://www.vulncheck.com/advisories/git-diff-before-2.0.7-os-command-injection-via-gitdiff-input-strings	none	yes	total
CVE-2026-110635	9,8	webp-converter	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	before 3.0.0	https://github.com/scionoftech/webp-converter https://github.com/scionoftech/webp-converter/blob/3729b65f1e904ab56b947ac3772020ce37a756c8/src/webpconverter.js#L41-L52 https://github.com/scionoftech/webp-converter/blob/e09d963d772cae9ff6af63c268ca838ab334f861/CHANGELOG.md https://github.com/scionoftech/webp-converter/commit/f1b6724bc2e89f67ab05d51a854b4b1c5a99928a https://github.com/scionoftech/webp-converter/pull/53 https://github.com/scionoftech/webp-converter/pull/53#issuecomment-5091652605			
CVE-2026-110638	9,8	doc-recog	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	through 1.1.6	https://github.com/zepspaiva/doc-recog https://github.com/zepspaiva/doc-recog/blob/96d31957fbc2a31f1d739e2d64e5c85a05f688ec/docdata.js#L69-L74 https://github.com/zepspaiva/doc-recog/pull/2 https://www.vulncheck.com/advisories/doc-recog-through-1.1.6-os-command-injection-via-docdata-readpdf-file-path			
CVE-2026-110639	9,8	@mborne/extract	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	before 0.2.1	https://github.com/mborne/node-extract/blob/v0.2.0/src/extractor/unzip.js#L17-L19 https://github.com/mborne/node-extract/commit/585e5b29657379e73c04f6f950ea8dc5319f8ae1 https://github.com/mborne/node-extract/pull/8 https://github.com/mborne/node-extract/releases/tag/v0.2.1 https://www.vulncheck.com/advisories/mborne-extract-before-0.2.1-os-command-injection-via-archivepath-and-targetdir	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-2026-110640	9,8	Whisper-node	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	through 1.1.1	https://github.com/arivm/whisper-node/blob/c72944cfa48f5c74662ff17ee2dc1d5f7624393e/src/whisper.ts#L58 https://github.com/arivm/whisper-node/blob/c72944cfa48f5c74662ff17ee2dc1d5f7624393e/src/whisper.ts#L8 https://github.com/arivm/whisper-node/pull/64 https://unpkg.com/whisper-node@1.1.1/dist/index.js https://www.vulncheck.com/advisories/whisper-node-through-1.1.1-os-command-injection-via-filepath-and-language			
CVE-2026-110643	9,8	transcribe2texts	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	through 1.0.6	https://github.com/kky-ykk/Transcribe2texts/blob/7e82f96466fed9ccfc40f7b9e370321701b82c32/lib/index.js#L53-L55 https://github.com/kky-ykk/Transcribe2texts/pull/1 https://www.vulncheck.com/advisories/transcribe2texts-through-1.0.6-os-command-injection-via-transcribeaudio-audiopath			
CVE-2026-110644	9,8	nodejs-whisper	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	through 0.3.1	https://github.com/ChetanXpro/nodejs-whisper/blob/v0.3.1/src/utils.ts#L58-L59 https://github.com/ChetanXpro/nodejs-whisper/blob/v0.3.1/src/utils.ts#L76-L77 https://github.com/ChetanXpro/nodejs-whisper/pull/259 https://www.vulncheck.com/advisories/nodejs-whisper-through-0.3.1-os-command-injection-via-converttowavtype	none	yes	total
CVE-2026-110649	9,8	Stills	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	before 25.24.2	https://github.com/shahkashani/stills/blob/66d5def1265b817d84524473a2813e4781dcbd80/lib/content/video.js#L58-L60 https://github.com/shahkashani/stills/blob/66d5def1265b817d84524473a2813e4781dcbd80/lib/stills/frames.js#L106-L108 https://github.com/shahkashani/stills/commit/51ba953983ba99915331607bf8530e6089952253 https://github.com/shahkashani/stills/commit/5694b3b0dcd2da342f4f0497244129d4c9eb73bc https://github.com/shahkashani/stills/pull/29 https://github.com/shahkashani/stills/pull/30	none	yes	total
CVE-2026-110911	9,8	Wheels	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.1.8 through 4.1.1; 4.0.0 through 4.1.1	https://github.com/wheels-dev/wheels/security/advisories/GHSA-96rm-h22v-925x	none	yes	total
CVE-2026-76519	9,8	the Advanced Malware Protection (AMP) feature of Cisco Secure Email Gateway	Relative Path Traversal	versions from (including) 15.0 up to (excluding) 15.5.5-014; versions from (including) 16.0 up to (excluding) 16.5.0-780	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-zqYJkjxp	active	yes	total
CVE-2026-110136	9,6	PDF in Google Chrome	Use After Free	prior to 155.0.8059.79	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01668083673.html	none	no	total
CVE-2026-110142	9,6	FileSystem in Google Chrome	Use After Free	prior to 155.0.8059.79	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01668083673.html	none	no	total
CVE-2026-110149	9,6	Browser in Google Chrome	Use After Free	prior to 155.0.8059.79	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01668083673.html	none	no	total
CVE-2026-110152	9,6	ANGLE in Google Chrome on on Android	Heap-based Buffer Overflow	prior to 155.0.8059.79	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01668083673.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-2026-110159	9,6	Updater in Google Chrome	Incorrect Authorization	prior to 155.0.8059.79	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01668083673.html	none	no	total
CVE-2026-110161	9,6	Network in Google Chrome	Use After Free	prior to 155.0.8059.79	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01668083673.html	none	no	total
CVE-2026-110165	9,6	Core in Google Chrome on on An-droid	Use After Free	prior to 155.0.8059.79	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01668083673.html	none	no	total
CVE-2026-99999	9,3	Linux		f43798c27684ab925ade7d8acc34c78c6e50df8 prior to a464d950f31c89565cbaae038cc60db04fe01956; f43798c27684ab925ade7d8acc34c78c6e50df8 prior to 0fab003ef4698e0628060a45a48f14b43ba2a40a; f43798c27684ab925ade7d8acc34c78c6e50df8 prior to 94524b7b32691de2e2ce162c04d6cbc9106e5cbf; f43798c27684ab925ade7d8acc34c78c6e50df8 prior to a65f69e0f38ffbed1b128029e09097436416dc8b; f43798c27684ab925ade7d8acc34c78c6e50df8 prior to 32a8b0adaa18e52aaa0b246b5ffe683075354dbb; f43798c27684ab925ade7d8acc34c78c6e50df8 prior to f3e835af6226f1dd12160cbd696081e9b6155de0; f43798c27684ab925ade7d8acc34c78c6e50df8 prior to c3e33464746166264334641dc850a36eef7e6326; f43798c27684ab925ade7d8acc34c78c6e50df8 prior to 6785011f8b16abf40b1e9d8b2e332232b3e68822; 2.6.27	https://git.kernel.org/stable/c/0fab003ef4698e0628060a45a48f14b43ba2a40a https://git.kernel.org/stable/c/32a8b0adaa18e52aaa0b246b5ffe683075354dbb https://git.kernel.org/stable/c/6785011f8b16abf40b1e9d8b2e332232b3e68822 https://git.kernel.org/stable/c/94524b7b32691de2e2ce162c04d6cbc9106e5cbf https://git.kernel.org/stable/c/a464d950f31c89565cbaae038cc60db04fe01956 https://git.kernel.org/stable/c/a65f69e0f38ffbed1b128029e09097436416dc8b			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-55240	9,1	Tianji	Improper Neutralization of Special Elements Used in a Template Engine	Prior to 1.31.29	https://github.com/msgbyte/tianji/commit/132ff67907df897d222829ea8ad1a018ff74df48 https://github.com/msgbyte/tianji/releases/tag/v1.31.29 https://github.com/msgbyte/tianji/security/advisories/GHSA-5qrg-j3cr-3hpm			
CVE-2026-108426	8,8	Microsoft Office Word	Heap-based Buffer Overflow	16.0.1 prior to https://aka.ms/OfficeSecurityReleases; 16.0.1 prior to 16.0.14334.20974; 16.0.0 prior to 16.0.17932.21056	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-108426	none	no	total
CVE-2026-108444	8,8	Microsoft Office	Heap-based Buffer Overflow	16.0.1 prior to https://aka.ms/OfficeSecurityReleases; 1.0.0 prior to 16.114.26101123; 16.0.1 prior to 16.0.14334.20974; 16.0.0 prior to 16.0.17932.21056; 16.0.1 prior to 16.114.26101123; 16.0.0 prior to 16.114.26101123	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-108444	none	no	total
CVE-2026-108446	8,8	Microsoft Office Excel	Use After Free	16.0.1 prior to https://aka.ms/OfficeSecurityReleases; 1.0.0 prior to 16.114.26101123; 16.0.1 prior to 16.0.14334.20974; 16.0.0 prior to 16.0.17932.21056; 16.0.1 prior to 16.114.26101123; 16.0.0 prior to 16.114.26101123; 16.0.0.0 prior to 16.0.10417.20228	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-108446	none	no	total
CVE-2026-108452	8,8	Microsoft Office SharePoint	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16.0.0 prior to 16.0.20326.20190	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-108452	none	no	total
CVE-2026-110137	8,8	WebRTC in Google Chrome	Use After Free	prior to 155.0.8059.79	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01668083673.html	none	no	total
CVE-2026-110139	8,8	Media in Google Chrome	Use After Free	prior to 155.0.8059.79	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01668083673.html	none	no	total
CVE-2026-110140	8,8	V8 in Google Chrome	Access of Resource Using Incompatible Type ('Type Confusion')	prior to 155.0.8059.79	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01668083673.html	none	no	total
CVE-2026-110148	8,8	SVG in Google Chrome	Use After Free	prior to 155.0.8059.79	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01668083673.html	none	no	total
CVE-2026-110154	8,8	Canvas in Google Chrome	Use After Free	prior to 155.0.8059.79	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01668083673.html	none	no	total
CVE-2026-110155	8,8	PDFium in Google Chrome	Heap-based Buffer Overflow	prior to 155.0.8059.79	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01668083673.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-2026-110162	8,8	Desktop in Google Chrome	Use After Free	prior to 155.0.8059.79	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01668083673.html	none	no	total
CVE-2026-110163	8,8	DOM in Google Chrome	Use After Free	prior to 155.0.8059.79	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01668083673.html	none	no	total
CVE-2026-110166	8,8	Animation in Google Chrome	Heap-based Buffer Overflow	prior to 155.0.8059.79	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01668083673.html	none	no	total
CVE-2026-110914	8,8	Workers in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 155.0.8059.84	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01886704284.html https://issues.chromium.org/issues/563194341	none	no	total
CVE-2026-110915	8,8	Compositing in Google Chrome	Use After Free	prior to 155.0.8059.84	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01886704284.html https://issues.chromium.org/issues/556272421	none	no	total
CVE-2026-110922	8,8	Prerender in Google Chrome	Use After Free	prior to 155.0.8059.84	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01886704284.html https://issues.chromium.org/issues/568719351	none	no	total
CVE-2026-111380	8,8	FreeRDP	Integer Overflow or Wraparound	before 3.32.0	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-72qv-qcph-rfwf https://www.vulncheck.com/advisories/freerdp-3.29.0-before-3.32.0-heap-overflow-via-audin-apple-backends			
CVE-2026-54525	8,8	Markdown Preview Enhanced	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Prior to 0.8.28	https://github.com/shd101wyy/crossnote/commit/5588ca2121c3da43fe331575dc5cf4ef347b91ee https://github.com/shd101wyy/crossnote/pull/442 https://github.com/shd101wyy/crossnote/releases/tag/0.9.29 https://github.com/shd101wyy/vscode-markdown-preview-enhanced/commit/dcd80281c986293b93d9f1af34ced64dcb230c77 https://github.com/shd101wyy/vscode-markdown-preview-enhanced/pull/2318 https://github.com/shd101wyy/vscode-markdown-preview-enhanced/releases/tag/0.8.28	none	no	total
CVE-2026-110144	8,6	Mojo in Google Chrome on on Windows	Incorrect Authorization	prior to 155.0.8059.79	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01668083673.html	none	no	total
CVE-2026-95634	8,6	CAI Content Credentials	Server-Side Request Forgery (SSRF)	versions up to (excluding) 0.91.1; versions up to (excluding) 0.15.3; versions up to (excluding) 0.28.1	https://www.adobe.com/trust/security/products/content-credentials-sdk/apsb26-163.html	none	yes	total
CVE-2024-22031	8,5	rancher	Incorrect Authorization	2.8.0 prior to 2.9.9; 2.10.0 prior to 2.10.5; 2.11.0 prior to 2.11.1	https://bugzilla.suse.com/show_bug.cgi?id=CVE-2024-22031 https://github.com/rancher/rancher/security/advisories/GHSA-8h6m-wv39-239m	none	no	total
CVE-2026-110138	8,3	ShapeDetection in Google Chrome	Use After Free	prior to 155.0.8059.79	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01668083673.html	none	no	total
CVE-2026-110145	8,3	Passwords in Google Chrome	Use After Free	prior to 155.0.8059.79	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01668083673.html	none	no	total
CVE-2026-110156	8,3	Extensions in Google Chrome on on Mac	Use of Incorrectly-Resolved Name or Reference	prior to 155.0.8059.79	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01668083673.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-2026-103895	8,1	The miniOrange OTP Login, Verification and SMS Notifications plugin for WordPress	Improper Authentication	up to, and including, 5.5.8	https://plugins.trac.wordpress.org/browser/miniorange-otp-verification/tags/5.5.7/handler/forms/class-wploginform.php#L1050 https://plugins.trac.wordpress.org/browser/miniorange-otp-verification/tags/5.5.7/handler/forms/class-wploginform.php#L1170 https://plugins.trac.wordpress.org/browser/miniorange-otp-verification/tags/5.5.7/handler/forms/class-wploginform.php#L1519 https://plugins.trac.wordpress.org/browser/miniorange-otp-verification/tags/5.5.7/handler/forms/class-wploginform.php#L1573 https://plugins.trac.wordpress.org/browser/miniorange-otp-verification/tags/5.5.7/handler/forms/class-wploginform.php#L511 https://plugins.trac.wordpress.org/browser/miniorange-otp-verification?rev=3741261			
CVE-2026-104745	8,1	The Customer Email Verification for WooCommerce plugin for WordPress	Improper Privilege Management	up to, and including, 3.3.0.	https://plugins.trac.wordpress.org/browser/emails-verification-for-woocommerce/tags/3.3.0/includes/alg-wc-ev-functions.php#L331 https://plugins.trac.wordpress.org/browser/emails-verification-for-woocommerce/tags/3.3.0/includes/class-alg-wc-ev-core.php#L1258 https://plugins.trac.wordpress.org/browser/emails-verification-for-woocommerce/tags/3.3.0/includes/class-alg-wc-ev-core.php#L498 https://plugins.trac.wordpress.org/browser/emails-verification-for-woocommerce/tags/3.3.0/includes/class-alg-wc-ev-core.php#L784 https://plugins.trac.wordpress.org/changeset?reponame=&old=3744623%40emails-verification-for-woocommerce&new=3744623%40emails-verification-for-woocommerce https://www.wordfence.com/threat-intel/vulnerabilities/id/6df7b3ed-a1e3-4df9-828e-95530661e27a?source=cve			
CVE-2026-109221	8,1	The Groundhogg — CRM, Newsletters, and Marketing Automation plugin for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	up to, and including, 4.9.3	https://github.com/groundhoggwp/groundhogg/commit/e319e4a849bfbb07cccfbac8558ad6bf07a7fdc0 https://plugins.trac.wordpress.org/browser/groundhogg/tags/4.9.3/admin/tools/tools-page.php#L575 https://plugins.trac.wordpress.org/browser/groundhogg/tags/4.9.3/admin/tools/tools-page.php#L602 https://plugins.trac.wordpress.org/browser/groundhogg/tags/4.9.3/includes/background/import-contacts.php#L200 https://plugins.trac.wordpress.org/browser/groundhogg/tags/4.9.3/includes/classes/traits/file-box.php#L85 https://plugins.trac.wordpress.org/browser/groundhogg/tags/4.9.3/includes/classes/traits/file-box.php#L94			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-109447	8,1	The User Profile Builder – Beautiful User Registration Forms, User Profiles & User Role Editor plugin for WordPress	Improper Privilege Management	up to, and including, 4.0.3	https://plugins.trac.wordpress.org/browser/profile-builder/tags/4.0.3/admin/admin-functions.php#L400 https://plugins.trac.wordpress.org/browser/profile-builder/tags/4.0.3/features/email-confirmation/email-confirmation.php#L262 https://plugins.trac.wordpress.org/browser/profile-builder/tags/4.0.3/front-end/class-formbuilder.php#L736 https://plugins.trac.wordpress.org/browser/profile-builder/tags/4.0.3/front-end/class-formbuilder.php#L793 https://plugins.trac.wordpress.org/browser/profile-builder/tags/4.0.3/front-end/register.php#L91 https://plugins.trac.wordpress.org/changeset/3741133/profile-builder			
CVE-2026-110646	8,1	Beganovich snappdf	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	before 6.1.0	https://github.com/beganovich/snappdf/blob/v6.0.0/src/Snappdf.php#L280-L284 https://github.com/beganovich/snappdf/commit/5197bd3bcc4df44e17246dbceea9ce51eb390eae https://github.com/beganovich/snappdf/pull/54 https://github.com/beganovich/snappdf/releases/tag/v6.1.0 https://www.vulncheck.com/advisories/beganovich-snappdf-1.1.0-before-6.1.0-os-command-injection-on-windows-via-seturl			
CVE-2023-32198	8,0	steve	Improper Certificate Validation	0.2.0 prior to 0.2.1; 0.3.0 prior to 0.3.3; 0.4.0 prior to 0.4.4; 0.5.0 prior to 0.5.13	https://bugzilla.suse.com/show_bug.cgi?id=CVE-2023-32198 https://github.com/rancher/steve/security/advisories/GHSA-95fc-g4qj-mqmx	none	no	total
CVE-2026-104932	8,0	The Search Regex plugin for WordPress; version	Deserialization of Untrusted Data	3.5 and earlier	https://plugins.trac.wordpress.org/changeset?reponame=&new=3730910%40search-regex%2Ftags%2F3.5.1&old=3729403%40search-regex%2Ftags%2F3.5 https://www.wordfence.com/threat-intel/vulnerabilities/id/cb801c72-0e50-4df1-88cc-30f8037c6d3c?source=cve			
CVE-2026-105429	8,0	the NetBird client SSH configuration manager (client/ssh/config/manager	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'); Improper Encoding or Escaping of Output	versions 0.60.0 through 0.74.6	https://github.com/netbirdio/netbird/pull/6805 https://github.com/netbirdio/netbird/releases/tag/v0.74.7 https://github.com/netbirdio/netbird/security/advisories/GHSA-xmg2-v32j-x2hf			
CVE-2026-103821	7,8	Substance3D - Designer	Out-of-bounds Write	versions up to (excluding) 16.0.7	https://www.adobe.com/trust/security/products/substance3d-designer/apsb26-169.html	none	no	total
CVE-2026-108433	7,8	a security decision in Microsoft Office Word	Reliance on Untrusted Inputs in a Security Decision	16.0.1 prior to https://aka.ms/OfficeSecurityReleases; 1.0.0 prior to 16.114.26101123; 16.0.1 prior to 16.0.14334.20974; 16.0.0 prior to 16.0.17932.21056; 16.0.1 prior to 16.114.26101123; 16.0.0 prior to 16.114.26101123	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-108433	none	no	total
CVE-2026-110359	7,8	Hyland Desktop Host for Windows	Incorrect Default Permissions	before 25.1.1	https://github.com/JNDataRT/Vulns/blob/main/Advisories/2026/1.md	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-2026-110648	7,8	@offactory/compress-fonts	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	before 1.1.1	https://github.com/adamarcanov/compress-fonts/blob/7b07d20b3125a7bba8f933eeca21f5a09c8fb62a/index.js#L48 https://github.com/adamarcanov/compress-fonts/commit/12002e5866af2163cd34424baae5a53338951a5d https://github.com/adamarcanov/compress-fonts/pull/1 https://www.vulncheck.com/advisories/offactory-compress-fonts-before-1.1.1-os-command-injection-via-font-file-names			
CVE-2026-110746	7,8	TotalAV	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'); Relative Path Traversal	7.1.17 and earlier	https://github.com/lukehebe/Vulnerability-Disclosures/tree/main/TotalAV-7.1.17-LPE https://www.totalav.com/ https://github.com/lukehebe/Vulnerability-Disclosures/blob/main/TotalAV-7.1.17-LPE/TotalAV_LPE.c	poc	no	total
CVE-2026-14765	7,7	Epic Games Unreal Engine versions up to and including	Initialization of a Resource with an Insecure Default	up to and including 5.8.0	https://khaelkugler.com/blogs/meccha_chameleon.html https://takeonme.org/gcves/GCVE-1337-2026-00000000000000000000000000000000000000000000000000001011111111101111111111100000000000000000000000000000000000000000000000000

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-103896	7,5		Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	up to, and including, 2.34.5	https://plugins.trac.wordpress.org/browser/tenweb-speed-optimizer/tags/2.34.5/includes/WebPageCache/OptimizerWebPageCache.php#L190 https://plugins.trac.wordpress.org/browser/tenweb-speed-optimizer/tags/2.34.5/includes/WebPageCache/OptimizerWebPageCache.php#L205 https://plugins.trac.wordpress.org/browser/tenweb-speed-optimizer/tags/2.34.5/includes/WebPageCache/OptimizerWebPageCache.php#L312 https://plugins.trac.wordpress.org/browser/tenweb-speed-optimizer/tags/2.34.5/includes/WebPageCache/OptimizerWebPageValidations.php#L299 https://plugins.trac.wordpress.org/browser/tenweb-speed-optimizer/tags/2.34.8 https://www.wordfence.com/threat-intel/vulnerabilities/id/83e672e7-2483-46e9-ae16-a9e7ccc4bcb8?source=cve			
CVE-2026-103936	7,5	libp2p	Uncaught Exception; Improper Handling of Exceptional Conditions	Prior to 6.0.28	https://github.com/libp2p/js-libp2p/commit/68794c8e2e67d5f38da59e379dc051b2789e46f6 https://github.com/libp2p/js-libp2p/pull/3584 https://github.com/libp2p/js-libp2p/releases/tag/webrtc-v6.0.28 https://github.com/libp2p/js-libp2p/security/advisories/GHSA-x3m2-6mq8-vj7f			
CVE-2026-107659	7,5	The Modula Image Gallery – Photo Grid & Video Gallery plugin for WordPress	Missing Authorization	up to, and including, 3.0.11	https://plugins.trac.wordpress.org/browser/modula-best-grid-gallery/ https://plugins.trac.wordpress.org/browser/modula-best-grid-gallery/tags/3.0.11/includes/admin/cpt/class-modula-cpt.php#L141 https://plugins.trac.wordpress.org/browser/modula-best-grid-gallery/tags/3.0.11/includes/admin/cpt/class-modula-cpt.php#L189 https://plugins.trac.wordpress.org/browser/modula-best-grid-gallery/tags/3.0.11/includes/admin/cpt/class-modula-cpt.php#L209 https://plugins.trac.wordpress.org/changeset/3729079/modula-best-grid-gallery/trunk/includes/admin/cpt/class-modula-cpt.php https://www.wordfence.com/threat-intel/vulnerabilities/id/ea70ffaf-b78b-4550-b334-d105f25b3f61?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-2026-107746	7,5	The FunnelKit – Funnel Builder for WooCommerce Checkout plugin for WordPress	Missing Authorization	up to, and including, 3.16.0.6	https://downloads.wordpress.org/plugin/funnel-builder.3.17.0.zip https://plugins.trac.wordpress.org/browser/funnel-builder/tags/3.16.0.5/modules/thankyou-pages/class-wffn-thank-you-wc-pages.php#L429 https://plugins.trac.wordpress.org/browser/funnel-builder/tags/3.16.0.5/modules/thankyou-pages/includes/class-wfty-data.php#L286 https://plugins.trac.wordpress.org/browser/funnel-builder/tags/3.16.0.5/modules/thankyou-pages/includes/class-wfty-data.php#L318 https://plugins.trac.wordpress.org/browser/funnel-builder/tags/3.16.0.5/modules/thankyou-pages/includes/class-wfty-data.php#L328 https://www.wordfence.com/threat-intel/vulnerabilities/id/bc9883b7-ea99-41e4-adf6-a3988f616a3f?source=cve			
CVE-2026-108395	7,5	The Model Context Protocol Java SDK	Allocation of Resources Without Limits or Throttling	From version 0.8.0 through 0.12.0; from 0.13.0 through 0.18.3; through 1.1.3; 2.0.0-M1 through 2.0.0	https://github.com/modelcontextprotocol/java-sdk/commit/1499df22c7023aa257223143a5dcf5b1db7ef80d https://github.com/modelcontextprotocol/java-sdk/commit/6a41dedaa0625551582d8247e5a4d78eae1131b2 https://github.com/modelcontextprotocol/java-sdk/commit/8c0fdd1b1f76adba3ce7945d29f73fa2ddc66598 https://github.com/modelcontextprotocol/java-sdk/commit/9e4d5fa827b6ba69457f5fd93573184789528efa https://github.com/modelcontextprotocol/java-sdk/releases/tag/v0.18.4 https://github.com/modelcontextprotocol/java-sdk/releases/tag/v1.1.4	none	yes	partial
CVE-2026-108448	7,5	Microsoft Office Outlook	Heap-based Buffer Overflow	16.0.1 prior to https://aka.ms/OfficeSecurityReleases; 1.0.0 prior to 16.114.26101123; 16.0.1 prior to 16.0.14334.20974; 16.0.0 prior to 16.0.17932.21056; 16.0.1 prior to 16.114.26101123; 16.0.0 prior to 16.114.26101123	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-108448	none	no	total
CVE-2026-109400	7,5	The InstaWP Connect –	Improper Privilege Management	up to, and including, 0.1.4.1	https://plugins.trac.wordpress.org/browser/instawp-connect/tags/0.1.4.1/admin/class-instawp-admin.php#L153 https://plugins.trac.wordpress.org/browser/instawp-connect/tags/0.1.4.1/includes/apis/class-instawp-rest-api.php#L663 https://plugins.trac.wordpress.org/browser/instawp-connect/tags/0.1.4.1/includes/class-instawp-hooks.php#L194 https://plugins.trac.wordpress.org/browser/instawp-connect/tags/0.1.4.1/includes/class-instawp-setting.php#L186 https://plugins.trac.wordpress.org/browser/instawp-connect/tags/0.1.4.1/includes/class-instawp-setting.php#L91 https://plugins.trac.wordpress.org/browser/instawp-connect/tags/0.1.4.1/includes/functions.php#L1041			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-109430	7,5	Ellucian WebAdvisor	Improper Restriction of XML External Entity Reference	3.2	https://www.ellucian.com/ https://www.vulncheck.com/advisories/ellucian-webadvisor-unauthenticated-xxe-injection			
CVE-2026-109468	7,5	ASP	Allocation of Resources Without Limits or Throttling	17.14.0 prior to 17.14.42; 18.10.0 prior to 18.10.4; 10.0.0 prior to 10.0.13	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-109468	none	no	partial
CVE-2026-110869	7,5	Nodemailer	Inefficient Regular Expression Complexity	before 10.0.13	https://github.com/nodemailer/nodemailer/security/advisories/GHSA-4ffr-jg9g-5ffx https://www.vulncheck.com/advisories/nodemailer-3.0.0-before-10.0.13-redos-via-smtp-auth-mechanism-detection-regexes	poc	yes	partial
CVE-2026-111114	7,5	The Nexter Extension – Security, Performance, Code Snippets & Site Toolkit plugin for WordPress	Improper Privilege Management	up to, and including, 4.7.11	https://plugins.trac.wordpress.org/browser/nexter-extension/tags/4.7.11/include/panel-settings/extensions/nexter-ext-view-admin-role.php#L265 https://plugins.trac.wordpress.org/browser/nexter-extension/tags/4.7.11/include/panel-settings/extensions/nexter-ext-view-admin-role.php#L287 https://plugins.trac.wordpress.org/browser/nexter-extension/tags/4.7.11/include/panel-settings/extensions/nexter-ext-view-admin-role.php#L302 https://plugins.trac.wordpress.org/browser/nexter-extension/tags/4.7.11/include/panel-settings/extensions/nexter-ext-view-admin-role.php#L51 https://plugins.trac.wordpress.org/changeset/3740891/nexter-extension/trunk/include/panel-settings/extensions/nexter-ext-view-admin-role.php https://www.wordfence.com/threat-intel/vulnerabilities/id/ae86441d-5a95-45a7-869a-9e7872365a1f?source=cve			
CVE-2026-95179	7,5	lottie-android	Uncontrolled Recursion	6.7.1 and earlier	https://github.com/FFG0d/security-advisories/blob/main/advisories/CVE-2026-95179.md https://github.com/Samsung/rlottie/pull/603 https://github.com/airbnb/lottie-android	none	yes	partial
CVE-2026-97370	7,5	Junrar	Loop with Unreachable Exit Condition ('Infinite Loop')	Prior to 7.6.1	https://github.com/junrar/junrar/commit/687a09c42f46066447faa9179ee11314ad6d9afb https://github.com/junrar/junrar/releases/tag/v7.6.1 https://github.com/junrar/junrar/security/advisories/GHSA-h9h9-2rmf-rvhp			
CVE-2026-111210	7,3	bitcoinj	Server-Side Request Forgery (SSRF)	up to 0.17.	https://github.com/bitcoinj/bitcoinj/ https://github.com/bitcoinj/bitcoinj/issues/4386 https://github.com/bitcoinj/bitcoinj/security/advisories/GHSA-cgq6-f9cp-chrp https://vuldb.com/cve/CVE-2026-111210 https://vuldb.com/submit/1004847 https://vuldb.com/vuln/420761			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-0322	7,2	PAN-OS	Improper Control of Generation of Code ('Code Injection')	versions up to (excluding) 10.2.0; versions from (including) 12.2.0 up to (excluding) 12.2.4; 10.2.7; 10.2.8; 10.2.9; 10.2.10; 10.2.11; 10.2.12; 10.2.13; 10.2.14; 10.2.15; 10.2.16; 10.2.17; 10.2.18; 11.1.0; 11.1.1; 11.1.2; 11.1.3; 11.1.4; 11.1.5; 11.1.6; 11.1.7; 11.1.8; 11.1.9; 11.1.10; 11.1.11; 11.1.12; 11.1.13; 11.1.14; 11.1.15; 11.1.16; 11.2.0; 11.2.1; 11.2.2; 11.2.3; 11.2.4; 11.2.5; 11.2.6; 11.2.7; 11.2.8; 11.2.9; 11.2.10; 11.2.11; 11.2.12; 11.2.13; 11.2.15; 12.1.2; 12.1.3; 12.1.4; 12.1.5; 12.1.6; 12.1.7; 12.1.8; 12.1.9; 12.1.10	https://security.paloaltonetworks.com/CVE-2026-0322	active	no	total
CVE-2026-103999	7,2	The Ultra Addons for Contact Form	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 3.5.54	https://downloads.wordpress.org/plugin/ultimate-addons-for-contact-form-7.zip https://plugins.trac.wordpress.org/browser/ultimate-addons-for-contact-form-7/tags/3.5.52/addons/database/database.php#L869 https://plugins.trac.wordpress.org/browser/ultimate-addons-for-contact-form-7/tags/3.5.52/addons/database/database.php#L895 https://plugins.trac.wordpress.org/browser/ultimate-addons-for-contact-form-7/tags/3.5.52/addons/database/database.php#L901 https://plugins.trac.wordpress.org/browser/ultimate-addons-for-contact-form-7/tags/3.5.52/inc/functions.php#L1703 https://plugins.trac.wordpress.org/changeset/3738548/ultimate-addons-for-contact-form-7/trunk/addons/database/database.php			
CVE-2026-104000	7,2	The Simply Schedule Appointments plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 1.6.12.35	https://plugins.trac.wordpress.org/browser/simply-schedule-appointments/tags/1.6.12.33/includes/class-appointment-model.php#L1490 https://plugins.trac.wordpress.org/browser/simply-schedule-appointments/tags/1.6.12.33/includes/class-debug.php#L92 https://plugins.trac.wordpress.org/browser/simply-schedule-appointments/tags/1.6.12.33/includes/class-utils.php#L716 https://plugins.trac.wordpress.org/changeset/3746344/simply-schedule-appointments/trunk/includes/class-appointment-model.php https://www.wordfence.com/threat-intel/vulnerabilities/id/3a8bd422-112c-43bc-a041-3c6eea27b790?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-2026-107764	7,2	The SiteOrigin CSS plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 1.6.7	https://github.com/siteorigin/so-css/compare/1.6.7...1.6.8 https://plugins.trac.wordpress.org/browser/so-css/tags/1.6.6/js/inspector.js#L280 https://plugins.trac.wordpress.org/browser/so-css/tags/1.6.6/so-css.php#L69 https://plugins.trac.wordpress.org/browser/so-css/tags/1.6.6/so-css.php#L899 https://www.wordfence.com/threat-intel/vulnerabilities/id/b0ff9652-1b45-43d6-949a-92bfeaee96d3?source=cve			
CVE-2026-109232	7,2	The Salon Booking System – Appointment Booking for Salons, Barbershops & Spas plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 10.31.9	https://plugins.trac.wordpress.org/browser/salon-booking-system/tags/10.31.9/src/SLN/Action/Init.php#L645 https://plugins.trac.wordpress.org/browser/salon-booking-system/tags/10.31.9/src/SLN/Form.php#L321 https://plugins.trac.wordpress.org/browser/salon-booking-system/tags/10.31.9/src/SLN/Shortcode/Salon/AbstractUserStep.php#L46 https://plugins.trac.wordpress.org/browser/salon-booking-system/tags/10.31.9/src/SLN/Shortcode/Salon/DetailsStep.php#L179 https://plugins.trac.wordpress.org/browser/salon-booking-system/tags/10.31.9/views/admin/_customer.php#L110 https://plugins.trac.wordpress.org/browser/salon-booking-system/tags/10.31.9/views/admin/_customer.php#L116			
CVE-2026-109513	7,2	NotificationX – FOMO, Live Sales Notification, WooCommerce Sales Popup, GDPR, Social Proof, Announcement Banner & Floating Notification Bar	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 3.3.3	https://plugins.trac.wordpress.org/browser/notificationx/tags/3.3.3/blocks/Blocks.php#L218 https://plugins.trac.wordpress.org/browser/notificationx/tags/3.3.3/includes/Core/Rest/Popup.php#L55 https://plugins.trac.wordpress.org/browser/notificationx/tags/3.3.3/includes/Extensions/PopupNotification/PopupNotification.php#L1119 https://plugins.trac.wordpress.org/browser/notificationx/tags/3.3.3/includes/Extensions/WordPress/WPOrgReview.php#L295 https://plugins.trac.wordpress.org/browser/notificationx/tags/3.3.3/includes/Features/ShortcodeInline.php#L148 https://plugins.trac.wordpress.org/changeset?reponame=&new=3746251%40notificationx%2Ftags%2F3.3.4&old=3720837%40notificationx%2Ftags%2F3.3.3			
CVE-2026-109990	7,2	The Flying Scripts: Delay JavaScript to Improve Site Speed & Performance plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 1.2.4	https://plugins.trac.wordpress.org/browser/flying-scripts/tags/1.2.4/html-rewrite.php#L36 https://plugins.trac.wordpress.org/browser/flying-scripts/tags/1.2.4/html-rewrite.php#L64 https://plugins.trac.wordpress.org/browser/flying-scripts/tags/1.2.4/lib/dom-parser.php#L2112 https://plugins.trac.wordpress.org/browser/flying-scripts/tags/1.2.4/lib/dom-parser.php#L2207 https://plugins.trac.wordpress.org/browser/flying-scripts/tags/1.2.4/lib/dom-parser.php#L2226 https://plugins.trac.wordpress.org/browser/flying-scripts/tags/1.2.4/lib/dom-parser.php#L497			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-89051	7,2	The WP Ghost (Hide My WP Ghost) – Security & Firewall plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 7.0.12	https://plugins.trac.wordpress.org/changeset?reponame=&new=3745418%40hide-my-wp%2Ftags%2F7.0.13&old=3726247%40hide-my-wp%2Ftags%2F7.0.12 https://www.wordfence.com/threat-intel/vulnerabilities/id/94724ff1-d3a7-4d9d-9423-a0e795360c95?source=cve			
CVE-2026-95686	7,2	The Opti-Behavior – Self-Hosted Heatmaps, Session Recordings, Funnels, A/B Testing & Smart Insights plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 1.9.2.1	https://plugins.svn.wordpress.org/opti-behavior/ https://plugins.trac.wordpress.org/browser/opti-behavior/tags/1.9.1/admin/class-opti-behavior-heatmap-ajax-handler.php#L1652 https://plugins.trac.wordpress.org/browser/opti-behavior/tags/1.9.1/admin/class-opti-behavior-heatmap-ajax-handler.php#L3455 https://plugins.trac.wordpress.org/browser/opti-behavior/tags/1.9.1/admin/class-opti-behavior-heatmap-post-metabox.php#L1389 https://plugins.trac.wordpress.org/browser/opti-behavior/tags/1.9.1/assets/js/metabox-analytics.js#L553 https://plugins.trac.wordpress.org/browser/opti-behavior/tags/1.9.1/public/class-opti-behavior-heatmap-frontend.php#L905			
CVE-2026-96570	7,2	The Schema & Structured Data for WP & AMP plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 1.67	https://plugins.trac.wordpress.org/browser/schema-and-structured-data-for-wp/tags/1.66/admin_section/common-function.php#L1874 https://plugins.trac.wordpress.org/browser/schema-and-structured-data-for-wp/tags/1.66/admin_section/common-function.php#L5158 https://plugins.trac.wordpress.org/browser/schema-and-structured-data-for-wp/tags/1.66/modules/reviews/class-saswp-reviews-admin.php#L159 https://plugins.trac.wordpress.org/browser/schema-and-structured-data-for-wp/tags/1.66/modules/reviews/class-saswp-reviews-admin.php#L258 https://plugins.trac.wordpress.org/browser/schema-and-structured-data-for-wp/tags/1.66/modules/reviews/class-saswp-reviews-form.php#L170 https://plugins.trac.wordpress.org/browser/schema-and-structured-data-for-wp/tags/1.66/modules/reviews/class-saswp-reviews-service.php#L126			
CVE-2026-97339	7,2	The Complianz GDPR/CCPA Cookie Consent Banner plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 7.5.5	https://plugins.trac.wordpress.org/browser/complianz-gdpr/tags/7.5.5/class-cookie-blocker.php#L458 https://plugins.trac.wordpress.org/browser/complianz-gdpr/tags/7.5.5/class-cookie-blocker.php#L828 https://plugins.trac.wordpress.org/browser/complianz-gdpr/tags/7.5.5/integrations/plugins/yotu-wp.php#L18 https://plugins.trac.wordpress.org/browser/complianz-gdpr/tags/7.5.5/integrations/plugins/yotu-wp.php#L7 https://plugins.trac.wordpress.org/changeset/3743098/complianz-gdpr/trunk/integrations/plugins/yotu-wp.php https://www.wordfence.com/threat-intel/vulnerabilities/id/3c12e65c-eedf-4fc2-977a-7a07219ee1c2?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-2026-9703	7,1	Grafana Enterprise; Grafana OSS	Improper Access Control	8.0.0 through 11.5.10; 11.6.0 through 11.6.16; 12.0.0 through 12.1.10; 12.2.0 through 12.2.10; 12.3.0 through 12.3.8; 12.4.0 through 12.4.5; 13.0.0 through 13.0.3; 8.0.0 through 12.3.0	https://grafana.com/security/security-advisories/cve-2026-9703			
CVE-2026-111357	7,0	Connect Secure	Inclusion of Functionality from Untrusted Control Sphere	22.8R2.4	https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-CVE-2026-104935 https://www.volexity.com/blog/2026/10/13/a-series-of-unauthenticated-events-chained-exploitation-of-ivanti-connect-secure-zero-days/	none	no	total

CISA/CERT-EU Alerts & Advisories

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

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds One Known Exploited Vulnerability to Catalog | CISA	▪ CVE-2026-21589 Atlassian Multiple Products Files or Directories Accessible to External Parties Vulnerability	https://cisa.gov/news-events/alerts/2026/10/15/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
Linus Torvalds Reveals Claude Code Wrote Linux Kernel Patches and Test Programs	https://cybersecuritynews.com/linus-torvalds-use-claude-code-patches
AI Slop Isn't Just for Social; It's Ruining Cyberattacks, Too	https://darkreading.com/threat-intelligence/ai-slop-ruining-cyberattacks
Android gets AI defenses against messaging scams, fake calls	https://bleepingcomputer.com/news/security/android-gets-ai-defenses-against-messaging-scams-fake-calls
Hackers hijack D-Link, Ubiquiti devices to resell your stolen bandwidth	https://bleepingcomputer.com/news/security/hackers-hijack-d-link-ubiquiti-devices-to-resell-your-stolen-bandwidth
Context Is King in the Fight Against Modern Cyberattacks	https://securityweek.com/context-is-king-in-the-fight-against-modern-cyberattacks

Watch Now: Zero Trust Strategies Summit - All Sessions Available on Demand	https://securityweek.com/virtual-event-today-zero-trust-strategies-summit-2
UK Legal Aid Agency Hack Scope Widens After Forensic Review	https://securityweek.com/uk-legal-aid-agency-hack-scope-widens-after-forensic-review
Just Viewing an Online Ad Can Infect Your Device With Spyware, Researchers Reveal	https://cybersecuritynews.com/0-click-spyware-infects-devices
France: Internet-Exposed Danfoss Controllers Drop 71% After Attack	https://infosecurity-magazine.com/news/france-expose-danfoss-controllers
Microsoft: Windows Server 2022 reached end of mainstream support	https://bleepingcomputer.com/news/microsoft/microsoft-windows-server-2022-reached-end-of-mainstream-support
Supermarket Refrigeration Attack Widens to Copeland, Dixell Controllers	https://securityweek.com/supermarket-refrigeration-attack-widens-to-copeland-dixell-controllers
Police arrests 95 suspects in international CSAM crackdown action	https://bleepingcomputer.com/news/security/police-arrests-95-suspects-in-child-sexual-abuse-material-crackdown
Microsoft Disrupts Global Yam Store Network Behind One Billion Phishin	https://infosecurity-magazine.com/news/microsoft-yam-store-one-billion
Anthropic Warns AI Agents Can Now Automate the Entire Cyber Kill Chain	https://cybersecuritynews.com/anthropic-warns-ai-agents
CISO Conversations: James Robinson – Many Jobs, One Journey to Netskope CISO	https://securityweek.com/ciso-conversations-james-robinson-many-jobs-one-journey-to-netskope-ciso
Privacy Policy	https://cybersecuritynews.com/privacy-policy-2
Article Publication and Retention Policy	https://cybersecuritynews.com/terms-of-service
About Us	https://cybersecuritynews.com/about-us
EU Grocers Pay a Steep Price for Unpatched Fridge Firmware	https://darkreading.com/ics-ot-security/eu-grocers-unpatched-fridge-firmware
FBI raids DPRK IT worker laptop farms in Texas, US nationals arrested	https://bleepingcomputer.com/news/security/fbi-raids-dprk-it-worker-laptop-farms-in-texas-us-nationals-arrested

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
Burger King Japan Confirms Data Breach Exposing 11.18M User Records	https://cybersecuritynews.com/burger-king-japan-data-breach
CenterPoint Energy Data Breach Impacts 1 Million Texans	https://securityweek.com/centerpoint-energy-data-breach-impacts-1-million-texans
ICO Reprimands Met Over Third-Party Data Leak	https://infosecurity-magazine.com/news/ico-reprimands-met-over-thirdparty
UK Legal Aid Agency: Hackers stole records dating back to 1978	https://bleepingcomputer.com/news/security/uk-legal-aid-agency-hackers-stole-records-dating-back-to-1978

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
Critical Adobe Acrobat Flaw Lets Malicious PDFs Trigger One-Click Memory Corruption	https://cybersecuritynews.com/adobe-acrobat-flaw
PoC Exploit Released for Critical GitLab RCE Vulnerability (CVE-2026-97229)	https://cybersecuritynews.com/poc-gitlab-rce-vulnerability
Critical Linux Kernel Flaw Lets Attackers Escape Virtual Machines and Take Control of Hosts	https://cybersecuritynews.com/linux-kernel-flaw-2
Critical PwnEscape Linux Kernel Vulnerability Lets Guest VMs Read Host Memory	https://thehackernews.com/2026/10/critical-pwnescape-linux-kernel.html
Silent Lynx Exploits WinRAR Flaw to Deploy Reverse Shell in CIS Government Attacks	https://thehackernews.com/2026/10/silent-lynx-exploits-winrar-flaw-to.html
Critical ChatGPT GitHub Connector Flaw Could Allow Attackers to Steal Private Repository Secrets	https://cybersecuritynews.com/chatgpt-github-connector-flaw
Citrix XenServer Vulnerabilities Could Allow Malicious VM Users to Compromise Host Systems	https://cybersecuritynews.com/citrix-xenserver-vulnerabilities
Critical Next.js Vulnerabilities Allow Hackers to Execute Malicious Code Remotely	https://cybersecuritynews.com/critical-next-js-vulnerabilities
Next.js Ships Out-of-Band Patch for Two Critical RCE Flaws in Caching and SVG Processing	https://thehackernews.com/2026/10/nextjs-ships-out-of-band-patch-for-two.html
Warning Over High-Risk Security Vulnerabilities in Widely Used LLM Gat	https://infosecurity-magazine.com/news/high-risk-vulnerabilities-llm-tool
Microsoft Windows Server 0-Day Flaw Lets Attackers Crash Servers With a Single Packet	https://cybersecuritynews.com/microsoft-windows-server-0-day-flaw
PoC Released for Critical Fortinet FortiClient EMS Authentication Bypass Vulnerability	https://cybersecuritynews.com/poc-released-for-forticlient-ems-vulnerability
Langflow's Critical Authenticated RCE Flaw Targeted in 1,423 Honeypot Exploit Attempts	https://thehackernews.com/2026/10/langflows-critical-authenticated-rce.html
AhsayCBS Flaws Exploited to Deploy Web Shells Get New Fixes After Incomplete Patches	https://thehackernews.com/2026/10/ahsaycbs-flaws-exploited-to-deploy-web.html
Cisco Warns of Exploited Secure Email Gateway Vulnerability	https://securityweek.com/cisco-warns-of-exploited-secure-email-gateway-vulnerability
Multiple Active Directory Vulnerabilities Let Attackers Bypass Security Feature Remotely	https://cybersecuritynews.com/multiple-active-directory-vulnerabilities
Hackers Exploit Palo Alto PAN-OS 0-day Flaw to Gain Root Code Execution on Firewalls	https://cybersecuritynews.com/pan-os-0-day-vulnerability
Cisco Secure Email Gateway 0-Day Vulnerability Actively Exploited in Attacks	https://cybersecuritynews.com/cisco-secure-email-gateway-0-day-vulnerability
Palo Alto Networks warns of PAN-OS RCE flaw exploited in attacks	https://bleepingcomputer.com/news/security/palo-alto-networks-warns-of-pan-os-rce-flaw-exploited-in-attacks
Ivanti Zero-Day Attacks Highlight Vendor Patching Hurdles	https://darkreading.com/vulnerabilities-threats/ivanti-ics-zero-day-attacks-vendor-patching

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
BeyondTrust patches zero-day exploited in attacks since August	https://bleepingcomputer.com/news/security/beyondtrust-patches-zero-day-exploited-in-attacks-since-august
NGINX Fixes 5 Flaws, Including Possible RCE and a TLS Bug That May Skip Client-Cert Checks	https://thehackernews.com/2026/10/nginx-fixes-5-flaws-including-possible.html
Drupal Patches Critical Field UI Flaw With Unauthenticated RCE Path via Contributed Modules	https://thehackernews.com/2026/10/drupal-patches-critical-core-rce-flaw.html
Palo Alto Networks Patches PAN-OS Authenticated RCE Flaw Amid Active Exploitation	https://thehackernews.com/2026/10/palo-alto-networks-patches-pan-os.html
Microsoft fixes bug causing Windows black screens, Explorer crashes	https://bleepingcomputer.com/news/microsoft/microsoft-fixes-bug-causing-windows-black-screens-explorer-crashes
Palo Alto Networks Patches PAN-OS Zero-Day Exploited for Remote Code Execution	https://securityweek.com/palo-alto-networks-patches-pan-os-zero-day-exploited-for-remote-code-execution
Cisco patches new Secure Email Gateway zero-day exploited in attacks	https://bleepingcomputer.com/news/security/cisco-patches-actively-exploited-secure-email-gateway-zero-day
Microsoft fixes VPN issues caused by September Windows updates	https://bleepingcomputer.com/news/microsoft/microsoft-fixes-vpn-issues-caused-by-september-windows-updates
curl Patches HTTP/2 Upload Flaw After PoC Demonstrates Client-Side Code Execution	https://thehackernews.com/2026/10/curl-patches-http2-upload-flaw-after.html
Microsoft Patches Record 1,413 Vulnerabilities, Including Exploited Windows Zero-Day	https://securityweek.com/microsoft-patches-record-1413-vulnerabilities-including-exploited-windows-zero-day
SAP Patches Critical NetWeaver, S/4HANA Vulnerabilities	https://securityweek.com/sap-patches-critical-netweaver-s-4hana-vulnerabilities
Microsoft Patches Record 1,413 Flaws, Including Exploited Windows Shell Bug	https://thehackernews.com/2026/10/microsoft-patches-record-1413-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. Περι-λαμβάνονται αναφορές σε εργαλεία που χρησιμοποιούν οι επιτιθέμενοι, αλλά και δείκτες (IoCs) που μπορούν να χρησιμοποιηθούν στην άμυνα.

Σύντομη περιγραφή / Τίτλος	URL
Hackers Target 60 Indian Banking and UPI Apps With New GhostBat Android Malware	https://cybersecuritynews.com/ghostbat-android-malware
PEERSTITCH Malware Deployed via FortiOS Flaw Bypasses Checks on Tagged VPN Sessions	https://thehackernews.com/2026/10/attackers-exploit-fortios-flaw-to.html
Hackers exploit Collabora RCE flaw to backdoor Nextcloud servers	https://bleepingcomputer.com/news/security/hackers-exploit-collabora-rce-flaw-to-backdoor-nextcloud-servers
ThreatsDay: Adobe RCE, DNS Wallet Theft, NVIDIA Container Escape, Self-Healing Backdoor + 23 More	https://thehackernews.com/2026/10/threatsday-adobe-rce-dns-wallet-theft.html
Fake Arch Linux packages push malware with root privileges	https://bleepingcomputer.com/news/security/fake-arch-linux-packages-push-malware-with-root-privileges
Hackers Use ClickFix and Python Tunnels to Prepare Systems for Ran-somware Attacks	https://cybersecuritynews.com/hackers-use-clickfix
Chinese Phishing Network Linked to 1 Billion Messages Targeting 75,000 Organizations	https://cybersecuritynews.com/chinese-phishing-network
New Aoki Infostealer Targets AI Coding Assistant Credentials	https://infosecurity-magazine.com/news/aoki-infostealer-ai-coding
Hackers Exploit Fortinet Vulnerabilities to Deploy Stealthy PEERSTITCH Malware on FortiGate Firewalls	https://cybersecuritynews.com/fortinet-vulnerabilities
CikaBika Bot RAT Uses Discord for C&C	https://securityweek.com/cikabika-bot-rat-uses-discord-for-cc
Novel Android RAT 'Hirudo' Replaces Banking Apps With Trojanized Copies	https://securityweek.com/novel-android-banking-rat-hirudo-replaces-banking-apps-with-trojanized-copies
Yam Store: The Phishing Network Behind a Billion Messages	https://darkreading.com/cyberattacks-data-breaches/yam-store-phishing-network-behind-billion-messages
Ledger asks sellers across Asia to halt sales after supply-chain attack	https://bleepingcomputer.com/news/security/ledger-asks-sellers-across-asia-to-halt-sales-after-supply-chain-attack
Hackers Backdoor Nextcloud Servers Through Critical Flaw in Collab-ora's Built-in CODE App	https://thehackernews.com/2026/10/hackers-backdoor-nextcloud-servers.html
ROMULUS Malware Server Leverages ClickFix to Deliver Multiple Pay-loads	https://infosecurity-magazine.com/news/romulus-malware-clickfix-deliver

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
Δεν εντοπίστηκαν άρθρα για το καθορισμένο χρονικό διάστημα.	

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 14/10/2026–16/10/2026, 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/