

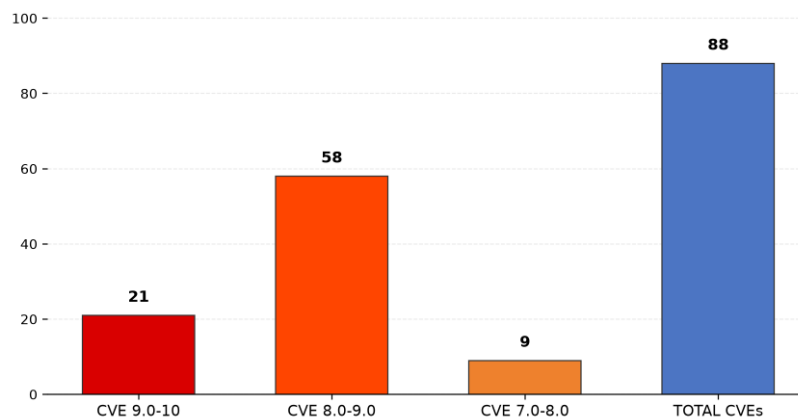


Newsletter on system vulnerabilities and
cybersecurity news.

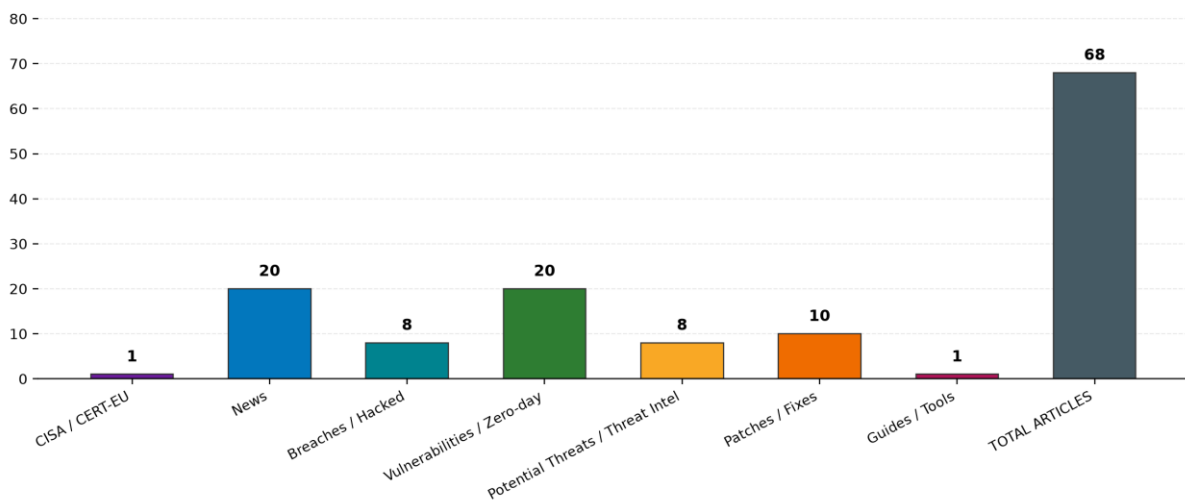
National Cyber Security Authority (NCSA)

Date: 21/10/2026 - 23/10/2026

of CVEs per CVSS score



of articles per section



Contents

Common Vulnerabilities and Exposures (CVEs)	3
CISA/CERT-EU Alerts & Advisories	8
News.....	9
Breaches / Compromised / Hacked.....	10
Vulnerabilities / Flaws / Zero-day.....	10
Patches / Updates / Fixes	11
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-2026-110063	10,0	VM Inspector for Azure Virtual Machines	Improper Link Resolution Before File Access ('Link Following')		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-110063	none	yes	total
CVE-2026-83938	10,0	Azure Kubernetes Configuration Service	Missing Authentication for Critical Function		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83938			
CVE-2022-51026	9,8	Bytebase	Authentication Bypass by Spoofing	before 1.0.1	https://github.com/bytebase/bytebase https://github.com/bytebase/bytebase/blob/1.0.0/server/auth.go#L79-L93 https://github.com/bytebase/bytebase/commit/d69e682243b25b51dd52912a26e2f259b5f3db2d https://github.com/bytebase/bytebase/pull/834 https://github.com/bytebase/bytebase/releases/tag/1.0.1 https://github.com/bytebase/bytebase/security/advisories/GHSA-5r3p-6r5-7937			
CVE-2026-113089	9,6	PrintPreview in Google Chrome	Improper Input Validation	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113116	9,6	DevTools in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113126	9,6	PolicyContainer in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113138	9,6	WebAppInstalls in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113169	9,6	WebAppInstalls in Google Chrome on Android	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113171	9,6	Prompts in Google Chrome on Android	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113189	9,6	Core in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113211	9,6	ServiceWorker in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113222	9,6	V8 in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113235	9,6	Passwords in Google Chrome	Improper Input Validation	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113252	9,6	ANGLE in Google Chrome on Windows	Improper Input Validation	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.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-2026-113263	9,6	Core in Google Chrome on on Android	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html https://issues.chromium.org/issues/497026542	none	no	total
CVE-2026-113270	9,6	Internals in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113283	9,6	CredentialProvider in Google Chrome on on Windows	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113300	9,6	Forms in Google Chrome	Out-of-bounds Write	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113328	9,6	Privacy in Google Chrome	Improper Input Validation	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113336	9,6	Compositing in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113342	9,6	Network in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113101	8,8	Sitelisolation in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113103	8,8	WebProtect in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113104	8,8	Frames in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113106	8,8	Skia in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113108	8,8	Script in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113110	8,8	ShadowDOM in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113114	8,8	SignIn in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113124	8,8	DataTransfer in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113133	8,8	PlatformIntegration in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113135	8,8	PictureInPicture in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113147	8,8	WebShare in Google Chrome	Improper Input Validation	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html https://issues.chromium.org/issues/501531546	poc	no	total
CVE-2026-113149	8,8	FullScreen in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113150	8,8	Bindings in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.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-2026-113155	8,8	Glic in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113161	8,8	WebRTC in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113165	8,8	Core in Google Chrome on on Mac	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113166	8,8	History in Google Chrome on on An-droid	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113173	8,8	UI in Google Chrome on on An-droid	Improper Input Validation	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113176	8,8	Omnibox in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113183	8,8	FedCM in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113184	8,8	Scheduling in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113187	8,8	DOM in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113191	8,8	Internals in Google Chrome on on Mac	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113195	8,8	Downloads in Google Chrome	Improper Input Validation	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113202	8,8	BrowserTag in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113204	8,8	TrustedWebActivities in Google Chrome on on An-droid	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113205	8,8	Variations in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113208	8,8	ContextualSearch in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113219	8,8	Contacts in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113221	8,8	Google Lens in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113226	8,8	Model in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113227	8,8	Editing in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113232	8,8	Search in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.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-2026-113236	8,8	Navigation in Google Chrome on on iOS	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113238	8,8	CustomTabs in Google Chrome on on Android	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html https://issues.chromium.org/issues/513789297	none	no	total
CVE-2026-113239	8,8	SiteIsolation in Google Chrome on on Android	Incorrect Access of Indexable Resource ('Range Error')	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113240	8,8	Chromecast in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113241	8,8	Toolbar in Google Chrome on on Android	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113244	8,8	UI in Google Chrome	Improper Input Validation	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113249	8,8	Mobile in Google Chrome on on iOS	Improper Input Validation	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html https://issues.chromium.org/issues/513480110	none	no	total
CVE-2026-113251	8,8	PDF in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113265	8,8	BFCache in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113266	8,8	ANGLE in Google Chrome on on Android	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113267	8,8	Video in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113271	8,8	Accessibility in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113274	8,8	ReadingMode in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113276	8,8	Passwords in Google Chrome on on Android	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html https://issues.chromium.org/issues/517809727	none	no	total
CVE-2026-113282	8,8	Views in Google Chrome on on Mac	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113284	8,8	XML in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113287	8,8	Prompts in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113312	8,8	Autofill in Google Chrome on on Mac	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113317	8,8	Accessibility in Google Chrome on on Mac	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113323	8,8	Chrome for iOS in Google Chrome on on iOS	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.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-2026-113331	8,8	Controls in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	poc	no	total
CVE-2026-113337	8,8	Scroll in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113339	8,8	SVG in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113343	8,8	Sandbox in Google Chrome	Improper Restriction of Operations within the Bounds of a Memory Buffer	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-113344	8,8	Performance in Google Chrome	Use After Free	prior to 156.0.8078.47	https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02018666648.html	none	no	total
CVE-2026-115414	7,8	the Terraform hook in AWS SAM CLI	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	before 1.166.2; 1.166.2 or later	https://aws.amazon.com/security/security-bulletins/2026-145-aws/ https://github.com/aws/aws-sam-cli/releases/tag/v1.166.2 https://github.com/aws/aws-sam-cli/security/advisories/GHSA-44mq-wirh-vpi6	none	no	total
CVE-2026-115504	7,8	CFITSIO	Out-of-bounds Write	through 4.7.0	https://gist.github.com/vure1432/98f15c7e8f48dc90ae65646f926aa176 https://github.com/HEASARC/cfitsio https://github.com/HEASARC/cfitsio/commit/579792e0f85bf0c6733ad5ebdf54c3b5c188686 https://github.com/HEASARC/cfitsio/pull/184 https://www.vulncheck.com/advisories/cfitsio-through-4.7.0-out-of-bounds-write-via-ffclcs2-in-getcols-c			
CVE-2026-13599	7,8	ABB Ability Edgenius	Missing Authentication for Critical Function	through 3.2.3.0.	https://search.abb.com/library/Download.aspx?DocumentID=7PAA026271&LanguageCode=en&DocumentPartId=&Action=Launch	none	no	total
CVE-2026-108456	7,7	Azure AI Foundry	Server-Side Request Forgery (SSRF)		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-108456			
CVE-2026-115484	7,6	the iscsiio component of open-iscsi	Out-of-bounds Read		https://access.redhat.com/security/cve/CVE-2026-115484 https://bugzilla.redhat.com/show_bug.cgi?id=2556265			
CVE-2026-115505	7,6	libsmb2	Integer Overflow or Wraparound	before 6.3	https://github.com/sahlberg/libsmb2 https://github.com/sahlberg/libsmb2/commit/a79f6914cb5ed3f74293d15cdea901261ce179ff https://github.com/sahlberg/libsmb2/issues/496 https://github.com/sahlberg/libsmb2/releases/tag/libsmb2-6.3 https://hackmd.io/@haindpwn/libsmb2-dcerpc-ndr-count-overflow-qob https://www.vulncheck.com/advisories/libsmb2-before-6.3-integer-overflow-in-dce-rpc-ndr-decoder-via-netshareenum			
CVE-2026-115497	7,5	The Music Store – WordPress eCommerce plugin for WordPress;	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	up to, and including, 1.4.7	https://plugins.trac.wordpress.org/browser/music-store/tags/1.4.7/ms-core/ms-download.php#L371 https://plugins.trac.wordpress.org/browser/music-store/tags/1.4.7/ms-core/ms-download.php#L378 https://plugins.trac.wordpress.org/browser/music-store/tags/1.4.7/ms-core/ms-download.php#L400 https://plugins.trac.wordpress.org/browser/music-store/tags/1.4.7/music-store.php#L312 https://plugins.trac.wordpress.org/browser/music-store/tags/1.4.8 https://www.wordfence.com/threat-intel/vulnerabilities/id/31e41b8c-f83f-4cd7-a30f-deac6154c7e3?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-2026-96185	7,5	Microsoft Exchange Online	Stack-based Buffer Overflow		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-96185	none	no	total
CVE-2026-109198	7,2	The Anti-Spam by CleanTalk – Spam Protection Without CAPTCHA plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 6.89.1	https://plugins.trac.wordpress.org/browser/cleantalk-spam-protect/tags/6.89.1/inc/cleantalk-public-integrations.php#L882 https://plugins.trac.wordpress.org/browser/cleantalk-spam-protect/tags/6.89.1/lib/Cleantalk/ApbctWP/FindSpam/ListTable/BadUsers.php#L87 https://plugins.trac.wordpress.org/browser/cleantalk-spam-protect/tags/6.89.1/lib/Cleantalk/ApbctWP/FindSpam/ListTable/Users.php#L113 https://plugins.trac.wordpress.org/browser/cleantalk-spam-protect/tags/6.89.1/lib/Cleantalk/ApbctWP/FindSpam/UsersChecker.php#L182 https://plugins.trac.wordpress.org/changeset?reponame=&old=3747972%40cleantalk-spam-protect&new=3747972%40cleantalk-spam-protect https://www.wordfence.com/threat-intel/vulnerabilities/id/93cf8a35-61a4-4998-ae34-86c96898e30f?source=cve			

CISA/CERT-EU Alerts & Advisories

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

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
Critical Vulnerabilities in PHP Require Immediate Patching CISA	• CVE-2026-109618 • CVE-2026-109619	https://cisa.gov/news-events/alerts/2026/10/21/critical-vulnerabilities-php-require-immediate-patching

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
Railway warns devs to rotate secrets after potential breach	https://bleepingcomputer.com/news/security/railway-warns-devs-to-rotate-secrets-after-potential-breach
Les supermarchés de l'UE paient	https://darkreading.com/ics-ot-security/eu-grocers-unpatched-fridge-firmware-french
eMudhra to Exit Global SSL/TLS Business After 8 Intermediate CA Keys Found Easily Guessable	https://thehackernews.com/2026/10/emudhra-to-exit-global-ssl-tls-business.html
Gcore Makes Enterprise Security Bundle Free for Public Agencies Until End of the Year	https://cybersecuritynews.com/gcore-makes-enterprise-security-bundle-free-for-public-agencies-until-end-of-the-year
Major U.S. Banks Detect Unauthorized AI Agents Operating Inside Customer Accounts	https://cybersecuritynews.com/u-s-banks-detect-unauthorized-ai-agents
A New Extortion Gang Is Naming Companies on the Dark Web and Counting Down to Data Leaks	https://cybersecuritynews.com/a-new-extortion-gang
Hacker Conversations: Corey Thuen and the Evil Bit	https://securityweek.com/hacker-conversations-corey-thuen-and-the-evil-bit
EU Regulators to Investigate Booking.com Over Scam Risks	https://infosecurity-magazine.com/news/eu-bookingcom-scam-risks
Indurex Raises \$8 Million to Expand Industrial Cybersecurity Platform	https://securityweek.com/indurex-raises-8-million-to-expand-industrial-cybersecurity-platform
Microsoft: Chinese State Actor Used AI to Compromise ConnectWise Tenan Privacy Policy	https://infosecurity-magazine.com/news/microsoft-chinese-ai-connectwise
Article Publication and Retention Policy	https://cybersecuritynews.com/terms-of-service
About Us	https://cybersecuritynews.com/about-us
PHP2Shell Exploitation Attempt Detected Four Days Before Disclosure	https://infosecurity-magazine.com/news/php2shell-exploitation-attempt
PHP2Shell Exploitation Started Days Before Patches	https://securityweek.com/php2shell-exploitation-started-days-before-patches
Authorities disrupt nearly 11,000 cybercrime networks in Africa	https://bleepingcomputer.com/news/security/authorities-disrupt-nearly-11-000-cybercrime-networks-in-africa
Cloud Security Maturity Lags Despite Widespread Adoption, SANS Warns	https://infosecurity-magazine.com/news/cloud-security-maturity-lags-sans
Meta Ordered to Pay New Mexico \$25 Billion for Deceiving Users About Privacy on Facebook	https://securityweek.com/meta-ordered-to-pay-new-mexico-25-billion-for-deceiving-users-about-privacy-on-facebook
UAE Transitions 50% of Gov't Services to Agentic AI	https://darkreading.com/cybersecurity-operations/uae-transitions-50-government-services-agentic-ai
Railway Security Incident: Hackers May Have Accessed Customer Environment Variables	https://cybersecuritynews.com/railway-security-incident

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
PwC Data Breach Claim - Everest Ransomware Group Claims to Have Stolen 590 GB of Data	https://cybersecuritynews.com/pwc-data-breach-claim
Quest Diagnostics Hacked - Attackers Accessed the System to Order Tests and View Results	https://cybersecuritynews.com/quest-diagnostics-hacked
Capcom confirms data breach affecting 11.7 million accounts	https://bleepingcomputer.com/news/security/capcom-confirms-data-breach-affecting-117-million-accounts
Japan's Onamae Desktop Cloud hacked, up to 27,000 servers affected	https://bleepingcomputer.com/news/security/japans-onamae-desktop-cloud-hacked-up-to-27-000-servers-affected
TiDB Breach Exposes Flawed Cloud Security Assumptions	https://darkreading.com/cloud-security/tidb-breach-flawed-cloud-security
SafePay Has Compromised 600 Critical Infrastructure Victims World-wide,	https://infosecurity-magazine.com/news/safepay-compromised-critical
SBI Confirms Data Breach - 3000+ Customer Records Exposed on Dark Web	https://cybersecuritynews.com/sbi-confirms-data-breach
Mozilla, Google, Apple block compromised eMudhra CA certificates	https://bleepingcomputer.com/news/security/mozilla-google-apple-block-compromised-emudhra-ca-certificates

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
Oracle Issues Emergency Java Update for Critical 9.1 HTTPS Trust Vulnerability	https://cybersecuritynews.com/emergency-java-update
Critical Cisco Expressway Vulnerability Enables Remote Code Execution Attacks	https://cybersecuritynews.com/critical-cisco-expressway-vulnerability
Arista Warns of Critical VeloCloud SQL Injection Zero-Day Exploited in Attacks	https://thehackernews.com/2026/10/arista-warns-of-critical-velocloud-sql.html
ThreatsDay: AI Secrets Leak, PingCAP Source Theft, Signal Hang-Up Flaw, Laravel Auth Bypass + 21 More	https://thehackernews.com/2026/10/threatsday-ai-secrets-leak-pingcap.html
Two CVSS 9.0 Linux KSMBD RCE Flaws Disclosed on Public Mailing Lists Before Kernel Fixes	https://thehackernews.com/2026/10/two-cvss-90-linux-ksmbd-rce-flaws.html
eMudhra Exits Global SSL/TLS Certificate Business Following the Vulnerability Disclosure	https://cybersecuritynews.com/emudhra-exits-global-ssl-tls-certificate
Claude Security Now Scans Repositories Continuously to Find Flaws and Track Fixes	https://cybersecuritynews.com/claude-security-continuous-scans

Hackers Were Targeting Critical PHP Vulnerabilities Days Before They Were Patched	https://cybersecuritynews.com/critical-php-vulnerabilities
Amazon says PHP2Shell exploitation began 4 days before patches	https://bleepingcomputer.com/news/security/amazon-says-php2shell-exploitation-began-4-days-before-patches
Signal Vulnerability Lets Malicious Callers Block Hang-Ups	https://securityweek.com/signal-vulnerability-lets-malicious-callers-block-hang-ups
Tech and Security Companies Respond to PHP2Shell Vulnerabilities	https://securityweek.com/tech-and-security-companies-respond-to-php2shell-vulnerabilities
GitLab warns of new max severity code execution vulnerability	https://bleepingcomputer.com/news/security/gitlab-warns-of-new-max-severity-code-execution-vulnerability
Splunk, SolarWinds Release Fresh Security Updates	https://securityweek.com/splunk-solarwinds-release-fresh-security-updates
OpenCode Flaw Lets Malicious MCP Servers Execute Code During Sign-In on Windows and WSL	https://thehackernews.com/2026/10/opencode-flaw-lets-malicious-mcp.html
Fortinet Urges Customers to Patch Critical Flaws Affecting FortiOS, FortiManager, and FortiAnalyzer	https://cybersecuritynews.com/fortinet-urges-to-patch-critical-flaws
Node.js Brotli Decoder Bug Could Allow Remote Code Execution in All Supported Versions	https://thehackernews.com/2026/10/nodejs-brotli-decoder-bug-could-allow.html
New QPACK Flaws Can Crash HTTP/3 Servers, Trigger Up to 4,000-Fold Memory Amplification	https://thehackernews.com/2026/10/new-qpack-flaws-can-crash-http3-servers.html
Someone Tried to Exploit PHP2Shell 4 Days Before the Vulnerabilities Were Publicly Disclosed	https://thehackernews.com/2026/10/someone-tried-to-exploit-php2shell-4.html
12-Year-Old GitLab Vulnerability Allows Remote Code Execution on Self-Managed Server	https://cybersecuritynews.com/12-year-old-gitlab-vulnerability
'PHP2Shell' Bugs Signal Red Alert for Security Industry	https://darkreading.com/application-security/php2shell-bugs-red-alert-security-industry

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
Splunk Fixes 24 Security Flaws, Including Four Critical Vulnerabilities in Enterprise and SOAR	https://cybersecuritynews.com/splunk-fixes-24-security-flaws
Critical Unpatched Linux Kernel Flaws Accidentally Disclosed on Public List	https://cybersecuritynews.com/linux-kernel-flaws-accidentally-disclosed
Arista patches new VeloCloud Orchestrator zero-day exploited in attacks	https://bleepingcomputer.com/news/security/arista-patches-new-velocloud-orchestrator-zero-day-exploited-in-attacks
Cisco Patches 34 Vulnerabilities Across Multiple Products	https://securityweek.com/cisco-patches-34-vulnerabilities-across-multiple-products
Oracle Patches Over 1,200 Vulnerabilities With October 2026 CPU	https://securityweek.com/oracle-patches-over-1200-vulnerabilities-with-october-2026-cpu
PHP2Shell Patches Land as First Exploitation Attempts Hit Sensors	https://securityweek.com/php2shell-patches-land-as-first-exploitation-attempts-hit-sensors
PHP Releases Emergency Patches for PHP2Shell Flaws Threatening Millions of Web Servers	https://cybersecuritynews.com/php-releases-emergency-patches

PHP ships emergency patches for critical PHP2Shell flaws	https://bleepingcomputer.com/news/security/php-ships-emergency-patches-for-critical-php2shell-flaws
PHP Issues Emergency Patches for Two Critical PHP2Shell RCE Flaws as Exploit Attempts Emerge	https://thehackernews.com/2026/10/php-issues-emergency-patches-for-two.html
PHP2Shell: Two Unpatched Critical PHP RCE Flaws (CVSS 9.2) Trigger Emergency Security Alert	https://thehackernews.com/2026/10/php2shell-two-unpatched-critical-php.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
LiteLLM release pipeline hacked to distribute info-stealer malware	https://bleepingcomputer.com/news/security/litellm-release-pipeline-hacked-to-distribute-info-stealer-malware
Iranian Hacking Group Found Hosting C2 Infrastructure in the US	https://infosecurity-magazine.com/news/iranian-hacking-group-hosting-c2
October 21 Cybersecurity Nightmare: PHP and Node.js Flaws, LiteLLM Backdoor, and Active Attacks	https://cybersecuritynews.com/october-21-cybersecurity-nightmare
Lazarus hackers use post-quantum cryptography for malware delivery	https://bleepingcomputer.com/news/security/lazarus-hackers-use-post-quantum-cryptography-for-malware-delivery
LiteLLM Compromised - Hackers Injected an Infostealer and RAT in the Latest 1.107.0 PyPI Release	https://cybersecuritynews.com/litellm-compromised
New PhaaS Platform Uses AI to Craft Phishing Lures and Mask Malicious	https://infosecurity-magazine.com/news/new-phaas-uses-ai-phishing-lures
Ransomware Attacks Rise as Rival Gangs Vie For Market Supremacy	https://infosecurity-magazine.com/news/rival-gangs-vie-for-market
Children's Data Stolen After Ransomware Attack Compromises 'Password1'	https://infosecurity-magazine.com/news/children-data-stolen-password1

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
Microsoft shares how to fix broken Exchange Online EWS apps	https://bleepingcomputer.com/news/microsoft/microsoft-shares-how-to-fix-broken-exchange-online-ews-apps

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 21/10/2026–23/10/2026, 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/