

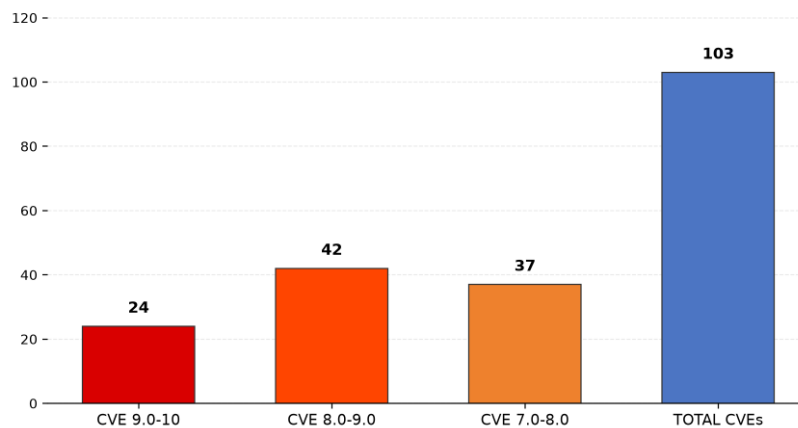


Newsletter on system vulnerabilities and cybersecurity news.

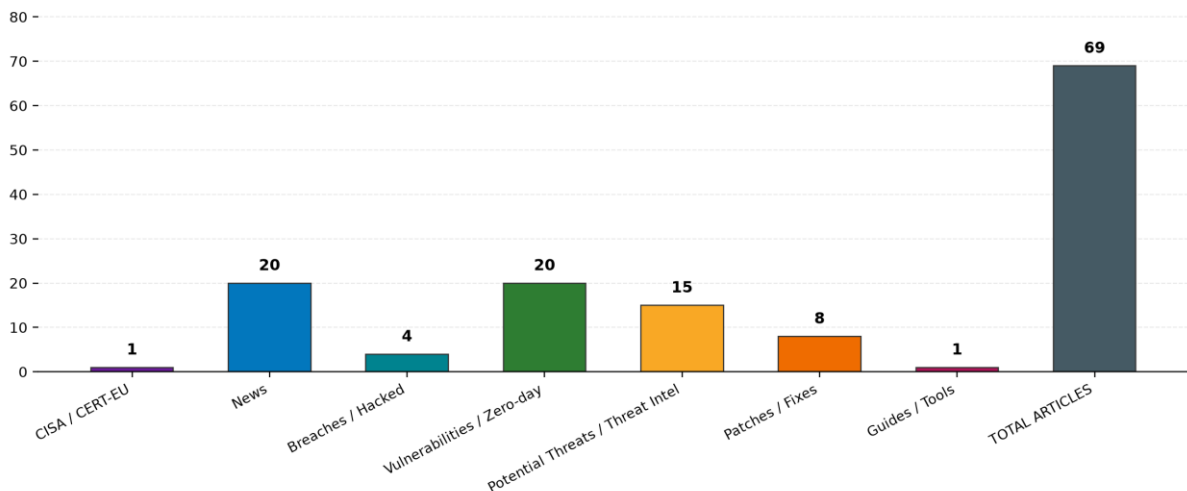
National Cyber Security Authority (NCSA)

Date: 16/09/2026 - 18/09/2026

of CVEs per CVSS score



of articles per section



Contents

Common Vulnerabilities and Exposures (CVEs)	3
CISA/CERT-EU Alerts & Advisories.....	26
News.....	26
Breaches / Compromised / Hacked.....	27
Vulnerabilities / Flaws / Zero-day.....	28
Patches / Updates / Fixes	29
Potential threats / Threat intelligence	29
Guides / Tools.....	30
References.....	31
Annex – Websites with vendor specific vulnerabilities	32

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-2026-54734	10,0	Prebid Server Java	Server-Side Request Forgery (SSRF)	Prior to 3.43.0	https://github.com/prebid/prebid-server-java/commit/a129a685b6fc54441c1a779ce29ea4ec20c2e09f https://github.com/prebid/prebid-server-java/commit/d0c723ce36aa09712c825ea9625d978f45d29a1c https://github.com/prebid/prebid-server-java/pull/4522 https://github.com/prebid/prebid-server-java/releases/tag/3.43.0 https://github.com/prebid/prebid-server-java/security/advisories/GHSA-fr2c-q2f8-qchq			
CVE-2026-62874	10,0	Azure Billing	Insufficient Verification of Data Authenticity		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62874			
CVE-2026-69843	10,0	Microsoft Fabric	Authentication Bypass by Spoofing		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69843			
CVE-2026-70200	10,0	Azure Logic Apps	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'); Improper Authorization		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70200			
CVE-2026-76460	10,0	an API of Cisco Identity Services Engine (ISE)	Incorrect Use of Privileged APIs	3.1.0; 3.2.0; 3.3.0; 3.4.0; 3.5.0	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-ABP-VNSW7Tn5	active	yes	total
CVE-2026-85889	10,0	Azure AI Foundry	Missing Authentication for Critical Function		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-85889			

CVE-2026-20332	9,9	Cisco Secure Firewall Adaptive Security Appliance (ASA) Software; Cisco Secure Firewall Management Center (FMC); Cisco Secure Firewall Threat Defense (FTD) Software	Improper Access Control	9.16.1; 9.16.1.28; 9.16.2; 9.16.2.3; 9.16.2.7; 9.16.2.11; 9.16.2.13; 9.16.2.14; 9.16.3.3; 9.16.3; 9.16.3.14; 9.16.3.15; 9.18.1.3; 9.18.2; 9.16.3.19; 9.16.3.23; 9.18.2.5; 9.16.4; 9.18.2.7; 9.16.4.9; 9.18.2.8; 9.16.4.14; 9.18.3; 9.16.4.18; 9.18.3.39; 9.16.4.19; 9.18.3.46; 9.16.4.27; 9.18.3.53; 9.18.3.55; 9.16.4.38; 9.16.4.39; 9.18.3.56; 9.20.1; 9.16.4.42; 9.18.4; 9.20.1.5; 9.18.4.5; 9.16.4.48; 9.18.4.8; 9.20.2; 9.16.4.55; 9.18.4.22; 9.20.2.10; 9.16.4.57; 9.18.4.24; 9.20.2.21; 9.16.4.61; 9.18.4.29; 9.20.2.22; 9.16.4.62; 9.18.4.34; 9.20.3; 9.16.4.67; 9.16.4.70; 9.18.4.40; 9.23.1; 9.22.1.1; 9.16.4.71; 9.20.3.4; 9.18.4.47; 9.20.3.7; 9.16.4.76; 9.20.3.9; 9.18.4.50; 9.22.1.3; 9.20.3.10; 9.22.1.2; 9.18.4.52; 9.20.3.13; 9.22.1.6; 9.18.4.53; 9.16.4.82; 9.22.2; 9.20.3.16; 9.19.1.42; 9.18.4.57; 9.16.4.84; 9.23.1.3; 9.20.3.20; 9.22.2.4; 9.23.1.7; 9.20.4; 9.22.2.9; 9.23.1.13; 9.20.4.7; 9.22.2.13; 9.18.4.66; 9.20.4.10; 9.23.1.19; 9.16.4.85; 9.22.2.14; 9.18.4.67; 9.24.1; 9.18.4.68; 9.23.1.22; 9.20.4.14; 9.22.2.20; 9.18.4.71; 9.20.4.19; 9.23.1.26; 9.16.4.89; 9.22.2.32; 9.18.4.76; 9.22.3; 9.24.1.5; 9.20.4.22; 9.24.1.9; 9.20.4.28; 9.22.3.5; 9.16.4.92; 9.18.4.135; 9.23.1.195; 9.20.4.30; 9.24.1.155; 9.23.1.32; 9.24.1.11; 9.20.4.34; 9.18.4.82; 9.24.10;	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-asatdftmc-uvpPROhN	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
				9.23.1.211; 9.20.4.235; 9.24.1.221; 9.22.3.191; 7.0.0; 7.0.0.1; 7.0.1; 7.0.1.1; 7.0.2; 7.2.0; 7.0.2.1; 7.0.3; 7.2.0.1; 7.0.4; 7.2.1; 7.0.5; 7.3.0; 7.2.2; 7.3.1; 7.2.3; 7.2.3.1; 7.2.4; 7.0.6; 7.2.4.1; 7.2.5; 7.3.1.1; 7.4.0; 7.0.6.1; 7.2.5.1; 7.4.1; 7.2.6; 7.4.1.1; 7.0.6.2; 7.2.7; 7.2.5.2; 7.3.1.2; 7.2.8; 7.6.0; 7.4.2; 7.2.8.1; 7.0.6.3; 7.4.2.1; 7.2.9; 7.0.7; 7.7.0; 7.4.2.2; 7.2.10; 7.6.1; 7.4.2.3; 7.0.8; 7.6.2; 7.7.10; 7.2.10.1; 7.0.8.1; 7.6.2.1; 7.2.10.2; 7.7.10.1; 7.4.2.4; 7.4.3; 7.6.3; 7.7.11; 7.6.4; 10.0.0; 7.4.4; 7.4.5; 7.0.9; 7.2.11; 7.7.12; 7.6.5; 7.4.6; 10.0.1; 7.4.7				
CVE-2026-85878	9,9	Azure Database for PostgreSQL	Improper Authorization		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-85878			
CVE-2026-54617	9,8	GravitLauncher	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'); Exposure of Sensitive Information to an Unauthorized Actor; Insufficiently Protected Credentials	Prior to 5.7.12	https://github.com/GravitLauncher/Launcher/commit/8114a1d4cfbcaab4c1c337d921597805d71dee3b https://github.com/GravitLauncher/Launcher/releases/tag/v5.7.12 https://github.com/GravitLauncher/Launcher/security/advisories/GHSA-5q75-4771-2c2f			
CVE-2026-61560	9,8	`@zereight/mcp-gitlab`	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Prior to version 2.1.27; Version 2.1.27	https://github.com/zereight/qitlab-mcp/pull/482 https://github.com/zereight/qitlab-mcp/pull/554 https://github.com/zereight/qitlab-mcp/pull/622 https://github.com/zereight/qitlab-mcp/security/advisories/GHSA-cv3r-c5h8-f4g5	poc	yes	total
CVE-2026-89778	9,8	Linux		> 17	https://git.kernel.org/stable/c/68d4d3e78150c7ed7d1195af63ad1e6ace30c661 https://git.kernel.org/stable/c/85904076cece72ee3194646ad7ac8e6659d999aa https://git.kernel.org/stable/c/8b994ac5778a725982fd6a8a3afcaa068d4a93e3 https://git.kernel.org/stable/c/9c6eace8d07e90f038c89eb3b756d65a7e259d48 https://git.kernel.org/stable/c/ad3249cd9d4ba34bb8b1ff3956a4020dfdb5b0a https://git.kernel.org/stable/c/cd616aa0449a772a6956abf03358f0f31720580			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-89783	9,8	xfrm6_input_addr() when secpath		9473e1f631de339c50b de1e3bd09e1045fe90fd 5 prior to 91fc387f63c00ddfb5221 127a17bac97549a8343 ; 9473e1f631de339c50b de1e3bd09e1045fe90fd 5 prior to 68e8737fe8e72f085c60 8cff322b3d2de8340af1; 9473e1f631de339c50b de1e3bd09e1045fe90fd 5 prior to 8fe2c53fb81f5ad5be43 af2ad09583f7c78b4b77 ; 9473e1f631de339c50b de1e3bd09e1045fe90fd 5 prior to bdcda866c89f9a8b1ac- dabf02d26cde9fbc501d 8; 9473e1f631de339c50b de1e3bd09e1045fe90fd 5 prior to 48996649222e95008cd b98cd58579e3fc8e5ee0 6; 9473e1f631de339c50b de1e3bd09e1045fe90fd 5 prior to 0f679e0523dfff3fb554 336ceb874b0e51e9cd3; 9473e1f631de339c50b de1e3bd09e1045fe90fd 5 prior to 5f35a29a5eed3d80befd 32050843ac88dea3d61 a; 9473e1f631de339c50b de1e3bd09e1045fe90fd 5 prior to 5d9e3bf34fec9a5d237e 4b7cef4a707bc2e091bc ; 2.6.25	https://git.kernel.org/stable/c/0f679e0523dfff3fb554336ceb874b0e51e9cd3 https://git.kernel.org/stable/c/48996649222e95008cdb98cd58579e3fc8e5ee06 https://git.kernel.org/stable/c/5d9e3bf34fec9a5d237e4b7cef4a707bc2e091bc https://git.kernel.org/stable/c/5f35a29a5eed3d80befd32050843ac88dea3d61a https://git.kernel.org/stable/c/68e8737fe8e72f085c608cff322b3d2de8340af1 https://git.kernel.org/stable/c/8fe2c53fb81f5ad5be43af2ad09583f7c78b4b77			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-89990	9,8	ceph_mds_check_access() MDS session OPEN handling replaces mdsc->s_cap_auths under mdsc->mutex, freeing the previous array and its strings		596afb0b8933ba6ed7227adcc538db26feb25c74 prior to 729c1ff670ece6f3d4b1738365a0b2f90d487523; 38365a0b2f90d487523; 596afb0b8933ba6ed7227adcc538db26feb25c74 prior to ca5bfea2045ef2eb3305cf2a9d8da549b76c37d3; cf2a9d8da549b76c37d3; 596afb0b8933ba6ed7227adcc538db26feb25c74 prior to df1a97d5313fccadb08390306d49b194fb027392; 596afb0b8933ba6ed7227adcc538db26feb25c74 prior to a61c6ae1dae2611082b831b4aaa780878099c012; 6.10	https://git.kernel.org/stable/c/729c1ff670ece6f3d4b1738365a0b2f90d487523 https://git.kernel.org/stable/c/a61c6ae1dae2611082b831b4aaa780878099c012 https://git.kernel.org/stable/c/ca5bfea2045ef2eb3305cf2a9d8da549b76c37d3 https://git.kernel.org/stable/c/df1a97d5313fccadb08390306d49b194fb027392			
CVE-2026-87701	9,6	output used by a downstream component ('injection') in Azure Cosmos DB	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-87701			
CVE-2026-91710	9,6	WebAppInstalls in Google Chrome	Use After Free	prior to 153.0.8010.47	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0541751186.html	none	no	total
CVE-2026-91716	9,6	Auth in Google Chrome	Use After Free	prior to 153.0.8010.47	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0541751186.html	none	no	total
CVE-2026-91718	9,6	Core in Google Chrome	Use After Free	prior to 153.0.8010.47	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0541751186.html https://issues.chromium.org/issues/553133215	none	no	total
CVE-2026-91728	9,6	V8 in Google Chrome	Integer Overflow or Wraparound	prior to 153.0.8010.47	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0541751186.html	none	no	total
CVE-2026-91729	9,6	DigitalCredentials in Google Chrome	Use After Free	prior to 153.0.8010.47	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0541751186.html	none	no	total
CVE-2026-91738	9,6	ANGLE in Google Chrome	Improper Input Validation	prior to 153.0.8010.47	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0541751186.html	none	no	total
CVE-2026-70009	9,3	Azure Arc	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70009			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-20284	9,1	the SXP REST API of Cisco ISE	Improper Neutralization of Special Elements in Data Query Logic	3.1.0; 3.1.0 p1; 3.1.0 p3; 3.1.0 p2; 3.2.0; 3.1.0 p4; 3.1.0 p5; 3.2.0 p1; 3.1.0 p6; 3.2.0 p2; 3.1.0 p7; 3.3.0; 3.2.0 p3; 3.2.0 p4; 3.1.0 p8; 3.2.0 p5; 3.2.0 p6; 3.1.0 p9; 3.3 Patch 2; 3.3 Patch 1; 3.3 Patch 3; 3.4.0; 3.2.0 p7; 3.3 Patch 4; 3.4 Patch 1; 3.1.0 p10; 3.3 Patch 5; 3.3 Patch 6; 3.4 Patch 2; 3.3 Patch 7; 3.4 Patch 3; 3.5.0; 3.4 Patch 4; 3.3 Patch 8; 3.2 Patch 8; 3.5 Patch 1; 3.3 Patch 9; 3.2 Patch 9; 3.4 Patch 5; 3.5 Patch 3; 3.5 Patch 2; 3.3 Patch 10; 3.3 Patch 11; 3.4 Patch 6; 3.2 Patch 10; 3.1.0 p72; 3.1.0 p11	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-mult-vul-vmSsTLCo	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-2026-89786	9,1	ext4_read_in- line_dir() ext4_read_in- line_dir()		c4d8b0235aa98f8c26bf 94d308be3fdd2415457 2 prior to d1e7c186555ad65554f d2f2b02f5a539aa35ae4 8; c4d8b0235aa98f8c26bf 94d308be3fdd2415457 2 prior to 5fd20d4e50dd6e460b3 ea8e4396f8553d4526f8 f; c4d8b0235aa98f8c26bf 94d308be3fdd2415457 2 prior to 1a1dea633b724a1c042 dbcd1fed27f41091668 8; c4d8b0235aa98f8c26bf 94d308be3fdd2415457 2 prior to b060861f662d4826dc7 00a1c3584243bb3474cf e; c4d8b0235aa98f8c26bf 94d308be3fdd2415457 2 prior to 6702c7da86d8c8b88d0f c57166286e115ffeb8c0; c4d8b0235aa98f8c26bf 94d308be3fdd2415457 2 prior to 36bf17bb90cdf7a62349 9b624b05acde4d2feef5 ; c4d8b0235aa98f8c26bf 94d308be3fdd2415457 2 prior to 9333cc809f0a89e001b8 14155a6cb8903a6274d f; 3.10	https://git.kernel.org/stable/c/1a1dea633b724a1c042dbcd1fed27f410916688 https://git.kernel.org/stable/c/36bf17bb90cdf7a623499b624b05acde4d2feef5 https://git.kernel.org/stable/c/5fd20d4e50dd6e460b3ea8e4396f8553d4526f8f https://git.kernel.org/stable/c/6702c7da86d8c8b88d0fc57166286e115ffeb8c0 https://git.kernel.org/stable/c/9333cc809f0a89e001b814155a6cb8903a6274df https://git.kernel.org/stable/c/b060861f662d4826dc700a1c3584243bb3474cfe			
CVE-2026-47252	9,0	Anyquery	Improper Control of Generation of Code ('Code Injection')	Prior to 0.4.5	https://github.com/julien040/anyquery/commit/33769e03bd4b0f76d7a20a4188cce7153f6db1c9 https://github.com/julien040/anyquery/releases/tag/0.4.5 https://github.com/julien040/anyquery/security/advisories/GHSA-hnj8-hjv8-mawc	poc	no	total

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-17086	8,8	The ShortPixel Image Optimizer – Optimize Images, Convert WebP & AVIF plugin for WordPress	Deserialization of Untrusted Data	up to, and including, 6.5.5	https://plugins.trac.wordpress.org/browser/shortpixel-image-optimiser/tags/6.5.1/build/shortpixel/replacer2/src/Replacer.php#L259 https://plugins.trac.wordpress.org/browser/shortpixel-image-optimiser/tags/6.5.1/build/shortpixel/replacer2/src/Replacer.php#L402 https://plugins.trac.wordpress.org/browser/shortpixel-image-optimiser/tags/6.5.1/build/shortpixel/replacer2/src/Replacer.php#L425 https://plugins.trac.wordpress.org/browser/shortpixel-image-optimiser/tags/6.5.1/build/shortpixel/replacer2/src/Replacer.php#L429 https://plugins.trac.wordpress.org/browser/shortpixel-image-optimiser/tags/6.5.1/build/shortpixel/replacer2/src/Replacer.php#L446 https://plugins.trac.wordpress.org/browser/shortpixel-image-optimiser/tags/6.5.1/class/Controller/Optimizer/OptimizeAIController.php#L598			
CVE-2026-20340	8,8	Cisco Secure FMC Software	Deserialization of Untrusted Data	7.0.0; 7.0.0.1; 7.0.1; 7.0.1.1; 7.0.2; 7.2.0; 7.0.2.1; 7.0.3; 7.2.0.1; 7.0.4; 7.2.1; 7.0.5; 7.3.0; 7.2.2; 7.3.1; 7.2.3; 7.2.3.1; 7.2.4; 7.0.6; 7.2.4.1; 7.2.5; 7.3.1.1; 7.4.0; 7.0.6.1; 7.2.5.1; 7.4.1; 7.2.6; 7.4.1.1; 7.0.6.2; 7.2.7; 7.2.5.2; 7.3.1.2; 7.2.8; 7.6.0; 7.4.2; 7.2.8.1; 7.0.6.3; 7.4.2.1; 7.2.9; 7.0.7; 7.7.0; 7.4.2.2; 7.2.10; 7.6.1; 7.4.2.3; 7.0.8; 7.6.2; 7.7.10; 7.2.10.1; 7.0.8.1; 7.6.2.1; 7.2.10.2; 7.7.10.1; 7.4.2.4; 7.4.3; 7.6.3; 7.7.11; 7.6.4; 10.0.0; 7.4.4; 7.4.5; 7.0.9; 7.2.11; 7.7.12; 7.6.5; 7.4.6; 10.0.1; 7.4.7	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-multivulns-4PsnFwvx	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-2026-20344	8,8	the web-based management interface of Cisco Secure FMC Software	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7.0.0; 7.0.0.1; 7.0.1; 7.0.1.1; 7.0.2; 7.2.0; 7.0.2.1; 7.0.3; 7.2.0.1; 7.0.4; 7.2.1; 7.0.5; 7.3.0; 7.2.2; 7.3.1; 7.2.3; 7.2.3.1; 7.2.4; 7.0.6; 7.2.4.1; 7.2.5; 7.3.1.1; 7.4.0; 7.0.6.1; 7.2.5.1; 7.4.1; 7.2.6; 7.4.1.1; 7.0.6.2; 7.2.7; 7.2.5.2; 7.3.1.2; 7.2.8; 7.6.0; 7.4.2; 7.2.8.1; 7.0.6.3; 7.4.2.1; 7.2.9; 7.0.7; 7.7.0; 7.4.2.2; 7.2.10; 7.6.1; 7.4.2.3; 7.0.8; 7.6.2; 7.7.10; 7.2.10.1; 7.0.8.1; 7.6.2.1; 7.2.10.2; 7.7.10.1; 7.4.2.4; 7.4.3; 7.6.3; 7.7.11; 7.6.4; 10.0.0; 7.4.4; 7.4.5; 7.0.9; 7.2.11; 7.7.12; 7.6.5; 7.4.6; 10.0.1; 7.4.7	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-multivulns-4PsnFwvx	none	no	total
CVE-2026-20360	8,8	Cisco Nexus Dashboard	Exposure of Sensitive Information to an Unauthorized Actor	2.1(1d); 2.1(1e); 2.1(2d); 2.2(1h); 2.2(1e); 2.2(2d); 2.1(2f); 2.3(1c); 2.3(2b); 2.3(2c); 2.3(2d); 2.3(2e); 3.0(1f); 3.0(1i); 3.1(1k); 3.1(1l); 3.2(1e); 3.2(1i); 3.3(1a); 3.3(1b); 3.3(2b); 4.0(1i); 3.3(2g); 3.2(2f); 3.2(2g); 3.2(2m); 3.1(1n); 4.1(1g); 4.2.1	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-ndw1-psFvnrq	none	no	total
CVE-2026-54239	8,8	faustjs	Insufficient Verification of Data Authenticity; Authorization Bypass Through User-Controlled Key	Prior to 1.8.11	https://github.com/wpengine/faustis/commit/cda00de7290f9b178cb1652d30b4cdf5bb8688d0 https://github.com/wpengine/faustis/pull/2386 https://github.com/wpengine/faustis/security/advisories/GHSA-g6pm-r77q-qcv3			
CVE-2026-54504	8,8	MCP Documentation Server	Missing Authentication for Critical Function; Exposure of Resource to Wrong Sphere	>= 1.13.0, < 1.13.1	https://github.com/andrea9293/mcp-documentation-server/commit/37159d4e06b8ee50c3645b2496e3d3f6d32c47f9 https://github.com/andrea9293/mcp-documentation-server/pull/20 https://github.com/andrea9293/mcp-documentation-server/releases/tag/v1.13.1 https://github.com/andrea9293/mcp-documentation-server/security/advisories/GHSA-6f5r-5672-7277	poc	no	total
CVE-2026-63506	8,8	Tina	Authorization Bypass Through User-Controlled Key	< 1.1.4; < 15.0.1	https://github.com/tinacms/tinacms/commit/0a927a4f8d228dd05ee7ca4be32899bc190e73af https://github.com/tinacms/tinacms/pull/7168 https://github.com/tinacms/tinacms/releases/tag/@tinacms/auth@1.1.4 https://github.com/tinacms/tinacms/releases/tag/next-tinacms-azure@15.0.1 https://github.com/tinacms/tinacms/security/advisories/GHSA-g74q-6q2f-874x	poc	no	total

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-77614	8,8	Opencast	Session Fixation	< 19.7; >= 20.0, < 20.2	https://github.com/opencast/opencast/commit/c36652250a026afb7cf78b663950c702669f1d3f https://github.com/opencast/opencast/commit/ff84128c9b3bcbd79c28192d25929dab8fa185f https://github.com/opencast/opencast/releases/tag/19.7 https://github.com/opencast/opencast/releases/tag/20.2 https://github.com/opencast/opencast/security/advisories/GHSA-6f53-1p7x-qg7p	poc	no	total
CVE-2026-86801	8,8	To Do List Member	Missing Authentication for Critical Function	from 1.4 through 1.6	https://wpscan.com/vulnerability/baebde16-141c-4de4-8ecb-173c25bed40d/	none	no	total
CVE-2026-91709	8,8	ServiceWorker in Google Chrome	Access of Resource Using Incompatible Type ('Type Confusion')	prior to 153.0.8010.47	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0541751186.html	none	no	total
CVE-2026-91721	8,8	Internals in Google Chrome	Use After Free	prior to 153.0.8010.47	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0541751186.html	none	no	total
CVE-2026-91722	8,8	Input in Google Chrome	Use After Free	prior to 153.0.8010.47	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0541751186.html	none	no	total
CVE-2026-91731	8,8	Compositing in Google Chrome	Access of Resource Using Incompatible Type ('Type Confusion')	prior to 153.0.8010.47	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0541751186.html	none	no	total
CVE-2026-91736	8,8	DOM in Google Chrome	Use After Free	prior to 153.0.8010.47	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0541751186.html	none	no	total
CVE-2026-91737	8,8	PDF in Google Chrome	Use After Free	prior to 153.0.8010.47	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0541751186.html	none	no	total
CVE-2026-91741	8,8	CacheStorage in Google Chrome	Access of Resource Using Incompatible Type ('Type Confusion')	prior to 153.0.8010.47	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0541751186.html	none	no	total
CVE-2026-92137	8,8	Jenkins Robot Framework Plugin	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	6.2.2 and earlier	https://www.jenkins.io/security/advisory/2026-09-16/#SECURITY-3971	none	no	total
CVE-2026-92593	8,8	Craft CMS	Improper Control of Generation of Code ('Code Injection')	versions 5.10.0 through 5.10.12	https://github.com/craftcms/cms/security/advisories/GHSA-5imw-g85v-7iv2 https://www.vulncheck.com/advisories/craft-cms-5.10.0-before-5.10.13-authenticated-remote-code-execution	none	no	total
CVE-2026-92780	8,8	KnowStreaming	Missing Authorization	through 3.4.1	https://github.com/didi/KnowStreaming https://github.com/didi/KnowStreaming/blob/v3.4.0/km-rest/src/main/java/com/xiaojukeji/know/streaming/km/rest/interceptor/PermissionInterceptor.java#L46-L74 https://github.com/didi/KnowStreaming/issues/1263 https://www.vulncheck.com/advisories/knowstreaming-through-3.4.1-missing-authorization-on-the-rest-api	poc	no	total
CVE-2026-92788	8,8	Coze Studio	Incorrect Authorization	through 0.5.1	https://github.com/coze-dev/coze-studio https://github.com/coze-dev/coze-studio/blob/22275b1c2661d35344a7493cffe401e8cc61cf8e/backend/domain/memory/database/service/database_impl.go#L2203-L2250 https://github.com/coze-dev/coze-studio/blob/22275b1c2661d35344a7493cffe401e8cc61cf8e/backend/infra/rdb/impl/rdb/mysql.go#L825-L830 https://github.com/coze-dev/coze-studio/issues/2710 https://www.vulncheck.com/advisories/coze-studio-through-0.5.1-cross-tenant-database-access-via-workflow-sql-node	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-2026-92918	8,8	admin3	Insertion of Sensitive Information into Log File	through 3.0.0	https://github.com/LinYuanvi1/cve-request-poc/blob/master/admin3/C02_log_session_token_disclosure.py https://github.com/cibi/admin3 https://github.com/cibi/admin3/blob/3.0.0/admin3-server/src/main/java/tech/wetech/admin3/infra/service/DefaultSessionService.java https://github.com/cibi/admin3/blob/3.0.0/admin3-server/src/main/java/tech/wetech/admin3/sys/service/LogService.java https://github.com/cibi/admin3/blob/3.0.0/admin3-server/src/main/resources/data.sql https://www.vulncheck.com/advisories/admin3-through-3.0.0-session-token-disclosure-via-audit-log	poc	no	total
CVE-2026-20135	8,6	the TLS	Double Free	7.0.0; 7.0.0.1; 7.0.1; 7.0.1.1; 7.0.2; 7.2.0; 7.0.2.1; 7.0.3; 7.2.0.1; 7.0.4; 7.2.1; 7.0.5; 7.3.0; 7.2.2; 7.2.3; 7.3.1; 7.2.4; 7.0.6; 7.2.5; 7.2.4.1; 7.3.1.1; 7.4.0; 7.0.6.1; 7.2.5.1; 7.4.1; 7.2.6; 7.0.6.2; 7.4.1.1; 7.2.7; 7.2.5.2; 7.3.1.2; 7.2.8; 7.6.0; 7.4.2; 7.2.8.1; 7.0.6.3; 7.4.2.1; 7.2.9; 7.0.7; 7.7.0; 7.4.2.2; 7.2.10; 7.6.1; 7.4.2.3; 7.0.8; 7.6.2; 7.7.10; 7.7.11; 7.0.8.1; 7.6.2.1; 7.7.10.1; 7.4.2.4; 7.2.10.2; 7.4.3; 7.6.4; 7.4.4; 7.0.9; 7.2.11	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fts1.3-dos-dLxwFWqF	none	yes	partial

CVE-2026-20249	8,6	the certification authentication feature of Internet Key Exchange	Incorrect Type Conversion or Cast	9.16.1; 9.16.1.28; 9.16.2; 9.16.2.3; 9.16.2.7; 9.16.2.11; 9.16.2.13; 9.16.2.14; 9.16.3.3; 9.16.3; 9.16.3.14; 9.18.1; 9.16.3.15; 9.18.1.3; 9.18.2; 9.16.3.19; 9.16.3.23; 9.18.2.5; 9.16.4; 9.18.2.7; 9.19.1; 9.16.4.9; 9.18.2.8; 9.16.4.14; 9.18.3; 9.19.1.5; 9.16.4.18; 9.19.1.9; 9.18.3.39; 9.16.4.19; 9.19.1.12; 9.18.3.46; 9.16.4.27; 9.19.1.18; 9.18.3.53; 9.18.3.55; 9.16.4.38; 9.16.4.39; 9.18.3.56; 9.20.1; 9.16.4.42; 9.19.1.22; 9.18.4; 9.20.1.5; 9.18.4.5; 9.19.1.24; 9.16.4.48; 9.18.4.8; 9.20.2; 9.19.1.27; 9.16.4.55; 9.18.4.22; 9.20.2.10; 9.16.4.57; 9.19.1.28; 9.18.4.24; 9.20.2.21; 9.16.4.61; 9.19.1.31; 9.18.4.29; 9.20.2.22; 9.16.4.62; 9.18.4.34; 9.20.3; 9.16.4.67; 9.16.4.70; 9.18.4.40; 9.23.1; 9.22.1.1; 9.16.4.71; 9.20.3.4; 9.18.4.47; 9.20.3.7; 9.19.1.37; 9.16.4.76; 9.20.3.9; 9.19.1.38; 9.18.4.50; 9.22.1.3; 9.20.3.10; 9.22.1.2; 9.18.4.52; 9.20.3.13; 9.22.1.6; 9.18.4.53; 9.16.4.82; 9.22.2; 9.20.3.16; 9.19.1.42; 9.18.4.57; 9.16.4.84; 9.23.1.3; 9.20.3.20; 9.22.2.4; 9.23.1.7; 9.20.4; 9.22.2.9; 9.23.1.13; 9.20.4.7; 9.22.2.13; 9.18.4.66; 9.20.4.10; 9.23.1.19; 9.16.4.85; 9.22.2.14; 9.18.4.67; 9.24.1; 9.18.4.68; 9.23.1.22; 9.20.4.14; 9.22.2.20; 9.18.4.71; 9.20.4.19; 9.23.1.26; 9.16.4.89; 9.22.2.32; 9.18.4.76; 9.22.3; 9.24.1.5; 9.20.4.22; 9.24.1.9;	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafld-ikev2cert-dos-uWyc2xlv			
--------------------------------	-----	---	-----------------------------------	---	---	--	--	--

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
				9.20.4.28; 9.16.4.92; 9.18.4.135; 9.23.1.195; 9.20.4.30; 9.24.1.155; 9.23.1.32; 9.18.4.82; 7.0.0; 7.0.0.1; 7.0.1; 7.0.1.1; 7.0.2; 7.2.0; 7.0.2.1; 7.0.3; 7.2.0.1; 7.0.4; 7.2.1; 7.0.5; 7.3.0; 7.2.2; 7.2.3; 7.3.1; 7.2.4; 7.0.6; 7.2.5; 7.2.4.1; 7.3.1.1; 7.4.0; 7.0.6.1; 7.2.5.1; 7.4.1; 7.2.6; 7.0.6.2; 7.4.1.1; 7.2.7; 7.2.5.2; 7.3.1.2; 7.2.8; 7.6.0; 7.4.2; 7.2.8.1; 7.0.6.3; 7.4.2.1; 7.2.9; 7.0.7; 7.7.0; 7.4.2.2; 7.2.10; 7.6.1; 7.4.2.3; 7.0.8; 7.6.2; 7.7.10; 7.7.11; 7.0.8.1; 7.6.2.1; 7.7.10.1; 7.4.2.4; 7.2.10.2; 7.4.3; 7.6.4; 10.0.0; 7.4.4; 7.0.9; 7.2.11; 7.4.7				
CVE-2026-20295	8,6	the sftunnel inter-device communication protocol of Cisco Secure FMC Software and Cisco Secure FTD Software	Memory Allocation with Excessive Size Value	7.0.0; 7.0.0.1; 7.0.1; 7.0.1.1; 7.0.2; 7.2.0; 7.0.2.1; 7.0.3; 7.2.0.1; 7.0.4; 7.2.1; 7.0.5; 7.3.0; 7.2.2; 7.3.1; 7.2.3; 7.2.3.1; 7.2.4; 7.0.6; 7.2.4.1; 7.2.5; 7.3.1.1; 7.4.0; 7.0.6.1; 7.2.5.1; 7.4.1; 7.2.6; 7.4.1.1; 7.0.6.2; 7.2.7; 7.2.5.2; 7.3.1.2; 7.2.8; 7.6.0; 7.4.2; 7.2.8.1; 7.0.6.3; 7.4.2.1; 7.2.9; 7.0.7; 7.7.0; 7.4.2.2; 7.2.10; 7.6.1; 7.4.2.3; 7.0.8; 7.6.2; 7.7.10; 7.2.10.1; 7.0.8.1; 7.6.2.1; 7.2.10.2; 7.7.10.1; 7.4.2.4; 7.4.3; 7.6.3; 7.7.11; 7.6.4; 10.0.0; 7.4.4; 7.4.5; 7.0.9; 7.2.11; 7.7.12; 7.6.5; 7.4.6; 10.0.1	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmctfd-sftun-multivulns-WGVHOrN3	none	yes	partial

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-20352	8,6	the RADIUS feature of Cisco Identity Services Engine (ISE)	Improper Restriction of Operations within the Bounds of a Memory Buffer	3.2.0; 3.2.0 p1; 3.2.0 p2; 3.3.0; 3.2.0 p3; 3.2.0 p4; 3.2.0 p5; 3.2.0 p6; 3.3 Patch 2; 3.3 Patch 1; 3.3 Patch 3; 3.4.0; 3.2.0 p7; 3.3 Patch 4; 3.4 Patch 1; 3.3 Patch 5; 3.3 Patch 6; 3.4 Patch 2; 3.3 Patch 7; 3.4 Patch 3; 3.5.0; 3.4 Patch 4; 3.3 Patch 8; 3.2 Patch 8; 3.5 Patch 1; 3.3 Patch 9; 3.2 Patch 9; 3.4 Patch 5; 3.5 Patch 3; 3.5 Patch 2; 3.3 Patch 10; 3.3 Patch 11; 3.4 Patch 6; 3.2 Patch 10	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-RADIUS-dos-wR3hYPMw	none	yes	partial
CVE-2026-68791	8,6	Azure Machine Learning	Incorrect Authorization		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68791			
CVE-2026-76412	8,5	the remote diagnostics debugger of Cisco Secure FMC Software	CWE CATEGORY: Permissions, Privileges, and Access Controls	7.7.0; 7.7.10; 7.7.10.1; 7.7.11; 10.0.0; 7.7.12; 10.0.1	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc2-multivulns-HXqcqRG	none	no	total
CVE-2026-54597	8,3	ITFlow	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Prior to version 26.07	https://github.com/itflow-org/itflow/commit/63d86917ae0438548d21d4e28e4d3c55176f5cbf https://github.com/itflow-org/itflow/pull/1289 https://github.com/itflow-org/itflow/releases/tag/v26.07 https://github.com/itflow-org/itflow-security/advisories/GHSA-m63v-i7fw-hq2h			
CVE-2026-91712	8,3	Extensions in Google Chrome on Mac	Time-of-check Time-of-use (TOCTOU) Race Condition	prior to 153.0.8010.47	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0541751186.html	none	no	total
CVE-2026-91733	8,3	Skia in Google Chrome	Improper Check for Unusual or Exceptional Conditions	prior to 153.0.8010.47	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0541751186.html	none	no	total
CVE-2026-91735	8,3	WebUI in Google Chrome	Incorrect Authorization	prior to 153.0.8010.47	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0541751186.html	none	no	total
CVE-2026-92752	8,3	metasfresh	Authorization Bypass Through User-Controlled Key	c4c7766ef403eb470c9130031cf24cc33625ceed	https://github.com/metasmfresh/metasmfresh https://github.com/metasmfresh/metasmfresh/blob/c4c7766ef403eb470c9130031cf24cc33625ceed/backend/de.metas.ui.web.base/src/main/java/de/metas/ui/web/attachments/DocumentAttachmentsRestController.java#L63-L225 https://github.com/metasmfresh/metasmfresh/blob/c4c7766ef403eb470c9130031cf24cc33625ceed/backend/de.metas.ui.web.base/src/main/java/de/metas/ui/web/upload/ImageRestController.java#L100-L107 https://github.com/metasmfresh/metasmfresh/issues/24665 https://www.vulncheck.com/advisories/metasmfresh-unauthorized-access-via-document-attachments-and-comments-endpoints			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-54354	8,2	MapServer	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Prior to 8.6.4	https://github.com/MapServer/MapServer/commit/65f1b53c258df2abdf6ce1f437c29e75e9976247 https://github.com/MapServer/MapServer/commit/bd59d49779d2ecc64ca8dc1281c53231a50b698e https://github.com/MapServer/MapServer/pull/7516 https://github.com/MapServer/MapServer/releases/tag/rel-8-6-4 https://github.com/MapServer/MapServer/security/advisories/GHSA-xp29-8wp5-wc3p https://mapserver.org/development/changelog/changelog-8-6.html#changelog-8-6			
CVE-2026-76413	8,2	Cisco Adaptive Security Device Manager (ASDM) single sign-on (SSO) handler for Cisco Secure FMC Software	Improper Restriction of Security Token Assignment	7.0.0; 7.0.0.1; 7.0.1; 7.0.1.1; 7.0.2; 7.2.0; 7.0.2.1; 7.0.3; 7.2.0.1; 7.0.4; 7.2.1; 7.0.5; 7.3.0; 7.2.2; 7.3.1; 7.2.3; 7.2.3.1; 7.2.4; 7.0.6; 7.2.4.1; 7.2.5; 7.3.1.1; 7.4.0; 7.0.6.1; 7.2.5.1; 7.4.1; 7.2.6; 7.4.1.1; 7.0.6.2; 7.2.7; 7.2.5.2; 7.3.1.2; 7.2.8; 7.6.0; 7.4.2; 7.2.8.1; 7.0.6.3; 7.4.2.1; 7.2.9; 7.0.7; 7.7.0; 7.4.2.2; 7.2.10; 7.6.1; 7.4.2.3; 7.0.8; 7.6.2; 7.7.10; 7.2.10.1; 7.0.8.1; 7.6.2.1; 7.2.10.2; 7.7.10.1; 7.4.2.4; 7.4.3; 7.6.3; 7.7.11; 7.6.4; 10.0.0; 7.4.4; 7.4.5; 7.0.9; 7.2.11; 7.7.12; 7.6.5; 7.4.6; 10.0.1; 7.4.7	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc2-multivulns-HXqcaRG	none	yes	partial
CVE-2026-83946	8,2	Azure Portal	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83946			
CVE-2026-92566	8,2	DataGear	Server-Side Request Forgery (SSRF)	through 6.0.0	https://github.com/datageartech/datagear https://github.com/datageartech/datagear/blob/fedefd4269b123e1e4f3e029906ed6e6f378c989/datagear-analysis/src/main/java/org/datagear/analysis/support/HttpDataSet.java#L386-L392 https://github.com/datageartech/datagear/blob/fedefd4269b123e1e4f3e029906ed6e6f378c989/datagear-web/src/main/java/org/datagear/web/config/CoreConfigSupport.java#L386-L390 https://github.com/datageartech/datagear/blob/fedefd4269b123e1e4f3e029906ed6e6f378c989/datagear-web/src/main/java/org/datagear/web/config/SecurityConfigSupport.java#L449-L453 https://github.com/datageartech/datagear/issues/37 https://www.vulncheck.com/advisories/datagear-through-6.0.0-unauthenticated-ssrf-via-http-dataset-preview	poc	yes	partial

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-92469	8,1	zlt2000 microservices-platform	Authorization Bypass Through User-Controlled Key	through 6.0.0	https://github.com/LinYuanyi/cve-request-poc/blob/master/microservice-platform/C19_delete_anv_file.py https://github.com/zlt2000/microservices-platform https://github.com/zlt2000/microservices-platform/blob/v6.0.0/zlt-business/file-center/src/main/java/com/central/file/controller/FileController.java#L48 https://www.vulncheck.com/advisories/microservices-platform-through-6.0.0-arbitrary-file-deletion-via-missing-ownership-check	poc	no	total
CVE-2026-92785	8,1	Angel	Deserialization of Untrusted Data	through 3.3.0	https://github.com/Angel-ML/angel https://github.com/Angel-ML/angel/blob/Release-3.3.0/angel-ps/core/src/main/java/com/tencent/angel/utis/KryoUtils.java#L45-L70 https://github.com/Angel-ML/angel/issues/1355 https://www.vulncheck.com/advisories/angel-through-3.3.0-unauthenticated-kryo-deserialization-of-arbitrary-classes	poc	no	total
CVE-2026-93393	8,1	the TLS transport layer of the MongoDB C Driver when built with the Windows platform TLS backend	Out-of-bounds Write	2.4.0; 2.3.0 through 2.3.3; 2.2.0 through 2.2.4; 2.1.0 through 2.1.2; 2.0.0 through 2.0.2; 1.30.0 through 1.30.8; 1.29.0 through 1.29.2; 1.28.0 through 1.28.1; 1.27.0 through 1.27.6; 1.26.0 through 1.26.2; 1.25.0 through 1.25.4; 1.24.0 through 1.24.4	https://ira.mongodb.org/browse/CDRIVER-6417			
CVE-2026-92134	8,0	Jenkins Warnings Plugin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13.10258.va_17d49a_78c3b_ and earlier	https://www.jenkins.io/security/advisory/2026-09-16/#SECURITY-3937	none	no	total
CVE-2026-92135	8,0	Jenkins Coverage Plugin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	3.3358.v9487dde48783 and earlier	https://www.jenkins.io/security/advisory/2026-09-16/#SECURITY-4118	none	no	total
CVE-2026-92136	8,0	Jenkins OWASP Dependency-Check Plugin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.6.4 and earlier	https://www.jenkins.io/security/advisory/2026-09-16/#SECURITY-3992	none	no	total
CVE-2026-10144	7,8	Rsbuild	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	before 2.0.9	https://github.com/web-infra-dev/rsbuild/commit/c1e2aebd6b1bbdaece15265572c3284f934b674d https://github.com/web-infra-dev/rsbuild/pull/7789 https://github.com/web-infra-dev/rsbuild/releases/tag/v2.0.9 https://www.vulncheck.com/advisories/rsbuild-command-injection-via-openbrowser-url-handling			
CVE-2026-86320	7,8	flatpak-builder where Git hooks	Improper Control of Generation of Code ('Code Injection')		https://access.redhat.com/security/cve/CVE-2026-86320 https://bugzilla.redhat.com/show_bug.cgi?id=2471023 https://github.com/flatpak/flatpak-builder/security/advisories/GHSA-j5n8-jqic-f3xv	poc	no	total

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκεύς/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-90009	7,8	io_uring passthrough command setup scsi_bsg_uring_cmd() reads bsg_uring_cmd from the shared mmap'd SQE		7b6d3255e7f8c6df2d21504c47808e3ce84649a c prior to f033530105aa73d82c121d54b57f358e4865d2f4; 7b6d3255e7f8c6df2d21504c47808e3ce84649a c prior to 4b3c5965fca99f62d31c963294bd5b23cc488e97; 7.1	https://git.kernel.org/stable/c/4b3c5965fca99f62d31c963294bd5b23cc488e97 https://git.kernel.org/stable/c/f033530105aa73d82c121d54b57f358e4865d2f4			
CVE-2026-20342	7,7	a specific file download API of Cisco Secure FMC Software	Authorization Bypass Through User-Controlled Key	7.0.0; 7.0.0.1; 7.0.1; 7.0.1.1; 7.0.2; 7.2.0; 7.0.2.1; 7.0.3; 7.2.0.1; 7.0.4; 7.2.1; 7.0.5; 7.3.0; 7.2.2; 7.3.1; 7.2.3; 7.2.3.1; 7.2.4; 7.0.6; 7.2.4.1; 7.2.5; 7.3.1.1; 7.4.0; 7.0.6.1; 7.2.5.1; 7.4.1; 7.2.6; 7.4.1.1; 7.0.6.2; 7.2.7; 7.2.5.2; 7.3.1.2; 7.2.8; 7.6.0; 7.4.2; 7.2.8.1; 7.0.6.3; 7.4.2.1; 7.2.9; 7.0.7; 7.7.0; 7.4.2.2; 7.2.10; 7.6.1; 7.4.2.3; 7.0.8; 7.6.2; 7.7.10; 7.2.10.1; 7.0.8.1; 7.6.2.1; 7.2.10.2; 7.7.10.1; 7.4.2.4; 7.4.3; 7.6.3; 7.7.11; 7.6.4; 10.0.0; 7.4.4; 7.4.5; 7.0.9; 7.2.11; 7.7.12; 7.6.5; 7.4.6; 10.0.1; 7.4.7	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-multivulns-4PsnFwvx	none	no	partial
CVE-2026-85887	7,7	M365 Copilot	Incorrect Permission Assignment for Critical Resource		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-85887			
CVE-2026-45726	7,6	a cloud	Exposure of Sensitive Information to an Unauthorized Actor; Insufficiently Protected Credentials; Incorrect Permission Assignment for Critical Resource	>= 1.3.0, < 1.6.6	https://github.com/siderolabs/omni/commit/25fa9e141e00285e70210ed40d11e4e457c871d https://github.com/siderolabs/omni/commit/a224cb020f3aaca2bc21c3e32a38eb4a37e531e8 https://github.com/siderolabs/omni/commit/b8ca100c4539ea83f0ac2e53dcd523e6e5b68111 https://github.com/siderolabs/omni/pull/2807 https://github.com/siderolabs/omni/releases/tag/v1.6.6 https://github.com/siderolabs/omni/releases/tag/v1.7.3			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-76425	7,6	the APIs of Cisco ISE	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	3.1.0; 3.1.0 p1; 3.1.0 p3; 3.1.0 p2; 3.2.0; 3.1.0 p4; 3.1.0 p5; 3.2.0 p1; 3.1.0 p6; 3.2.0 p2; 3.1.0 p7; 3.3.0; 3.2.0 p3; 3.2.0 p4; 3.1.0 p8; 3.2.0 p5; 3.2.0 p6; 3.1.0 p9; 3.3 Patch 2; 3.3 Patch 1; 3.3 Patch 3; 3.4.0; 3.2.0 p7; 3.3 Patch 4; 3.4 Patch 1; 3.1.0 p10; 3.3 Patch 5; 3.3 Patch 6; 3.4 Patch 2; 3.3 Patch 7; 3.4 Patch 3; 3.5.0; 3.4 Patch 4; 3.3 Patch 8; 3.2 Patch 8; 3.5 Patch 1; 3.3 Patch 9; 3.2 Patch 9; 3.4 Patch 5; 3.5 Patch 3; 3.5 Patch 2; 3.3 Patch 10; 3.3 Patch 11; 3.4 Patch 6; 3.2 Patch 10; 3.1.0 p72; 3.1.0 p11; 3.3 Patch 12	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-hrP9jOSQ	none	no	partial
CVE-2026-20247	7,5	Cisco ISE	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	3.1.0; 3.1.0 p1; 3.1.0 p3; 3.1.0 p2; 3.2.0; 3.1.0 p4; 3.1.0 p5; 3.2.0 p1; 3.1.0 p6; 3.2.0 p2; 3.1.0 p7; 3.3.0; 3.2.0 p3; 3.2.0 p4; 3.1.0 p8; 3.2.0 p5; 3.2.0 p6; 3.1.0 p9; 3.3 Patch 2; 3.3 Patch 1; 3.3 Patch 3; 3.4.0; 3.2.0 p7; 3.3 Patch 4; 3.4 Patch 1; 3.1.0 p10; 3.3 Patch 5; 3.3 Patch 6; 3.4 Patch 2; 3.3 Patch 7; 3.4 Patch 3; 3.5.0; 3.4 Patch 4; 3.3 Patch 8; 3.2 Patch 8; 3.5 Patch 1; 3.3 Patch 9; 3.2 Patch 9; 3.4 Patch 5; 3.5 Patch 3; 3.5 Patch 2; 3.3 Patch 10; 3.3 Patch 11; 3.4 Patch 6; 3.2 Patch 10; 3.1.0 p72; 3.1.0 p11	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-sql-inj-3QTKR947	none	yes	partial

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-20343	7,5	a critical API for Cisco Secure FMC Software	Missing Authentication for Critical Function	7.3.0; 7.3.1; 7.3.1.1; 7.4.0; 7.4.1; 7.4.1.1; 7.3.1.2; 7.6.0; 7.4.2; 7.4.2.1; 7.7.0; 7.4.2.2; 7.6.1; 7.4.2.3; 7.6.2; 7.7.10; 7.6.2.1; 7.7.10.1; 7.4.2.4; 7.4.3; 7.6.3; 7.7.11; 7.6.4; 10.0.0; 7.4.4; 7.4.5; 7.7.12; 7.6.5; 7.4.6; 10.0.1; 7.4.7	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-multivulns-4PsnFwwx			
CVE-2026-50125	7,5	MKP	Uncontrolled Resource Consumption	Prior to 0.4.1	https://github.com/StacklokLabs/mkp/commit/37bf6bac862aa3b1c71b8aa1b8364eae7818962d https://github.com/StacklokLabs/mkp/security/advisories/GHSA-qw5r-ppcq-l8rj			
CVE-2026-63126	7,5	Wire	Integer Overflow or Wraparound	Prior to 6.4.5 and 7.0.0-alpha04	https://github.com/square/wire/commit/082d5d83cec57ef68f1dd7d3e3d1d641c1fb670f https://github.com/square/wire/commit/25ebcabb9ab7f12d1d77af75ecbc51726fddc015 https://github.com/square/wire/pull/3635 https://github.com/square/wire/releases/tag/6.4.5 https://github.com/square/wire/releases/tag/7.0.0-alpha04 https://github.com/square/wire/security/advisories/GHSA-A9rm7-3qhh-h2mq	poc	yes	partial
CVE-2026-65388	7,5	containerization	URL Redirection to Untrusted Site ('Open Redirect')	prior to 0.41.0	https://github.com/apple/containerization/security/advisories/GHSA-mx96-5vvg-x2mq	none	yes	partial
CVE-2026-81875	7,5	HAPI FHIR; Java	Improper Input Validation; Uncontrolled Resource Consumption; Improper Handling of Highly Compressed Data (Data Amplification)	Prior to version 6.9.12	https://github.com/hapifhir/org.hl7.fhir.core/commit/fbb94216e0ad21ded75be77e5e20242ba194e83f https://github.com/hapifhir/org.hl7.fhir.core/pull/2493 https://github.com/hapifhir/org.hl7.fhir.core/releases/tag/6.9.11 https://github.com/hapifhir/org.hl7.fhir.core/releases/tag/6.9.12 https://github.com/hapifhir/org.hl7.fhir.core/security/advisories/GHSA-3w98-rprf-fprf	poc	yes	partial
CVE-2026-84997	7,5	react/http	Loop with Unreachable Exit Condition ('Infinite Loop')	>= 0.6.0, < 1.11.1	https://github.com/reactphp/http/commit/b6d4688790adf3797071cf88a3fc4225f30486a https://github.com/reactphp/http/releases/tag/v1.11.1 https://github.com/reactphp/http/security/advisories/GHSA-x424-64qh-5j54	poc	yes	partial
CVE-2026-85128	7,5	The Choose User Role at Registration WordPress plugin	Improper Privilege Management	before 1.3.3	https://wpscan.com/vulnerability/e48789a3-49b4-4fa4-8243-c242b79b9d9d/	none	no	total
CVE-2026-85715	7,5	ExifReader	Memory Allocation with Excessive Size Value; Loop with Unreachable Exit Condition ('Infinite Loop')	Prior to 4.41.1	https://github.com/mattiasw/ExifReader/commit/17b901cd192d2c90d7f9f347bd3073b28b482699 https://github.com/mattiasw/ExifReader/releases/tag/v4.41.1 https://github.com/mattiasw/ExifReader/security/advisories/GHSA-pi96-35fo-cfcc	poc	yes	partial

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-85719	7,5	The AsyncHttpClient (AHC) library	Cleartext Transmission of Sensitive Information; Insufficiently Protected Credentials	before 2.1.0	https://github.com/AsyncHttpClient/async-http-client/commit/4d887704dec22027310f66c81503226722e9bd23 https://github.com/AsyncHttpClient/async-http-client/commit/718ed2e86126663a88ea3db7a88cbbf93f0069b5 https://github.com/AsyncHttpClient/async-http-client/commit/abaa8bd260beda3b85825f95069ed11eaf4ca8d https://github.com/AsyncHttpClient/async-http-client/commit/be439b2ec773d12d61914c238d3e8eeaa6f0ba21 https://github.com/AsyncHttpClient/async-http-client/security/advisories/GHSA-x5w6-vm3f-pp6f			
CVE-2026-87742	7,5	quarkus-websockets-next	Allocation of Resources Without Limits or Throttling		https://access.redhat.com/security/cve/CVE-2026-87742 https://bugzilla.redhat.com/show_bug.cgi?id=2530522	none	yes	partial
CVE-2026-92596	7,5	Nodemailer	Uncontrolled Resource Consumption	before 9.1.0	https://github.com/nodemailer/nodemailer/commit/34da642 https://github.com/nodemailer/nodemailer/commit/7cc38af https://github.com/nodemailer/nodemailer/commit/83b8c48 https://github.com/nodemailer/nodemailer/commit/9116da9 https://github.com/nodemailer/nodemailer/security/advisories/GHSA-2x7j-588q-ccc2 https://www.vulncheck.com/advisories/nodemailer-before-9.1.0-denial-of-service-via-addressparser	poc	yes	partial
CVE-2026-92815	7,5	changedetection.io	Server-Side Request Forgery (SSRF)	through 0.60.6	https://github.com/dgtlmoon/changedetection.io https://github.com/dgtlmoon/changedetection.io/blob/0.60.6/changedetectionio/browser_steps/browser_steps.py#L182-L192 https://github.com/geo-chen/oss/blob/main/changedetection.io.md#finding-2-ssrf-via-browser-step-goto-url-action-bypasses-the-ssrf-guard-guard-only-applied-to-the-main-watch-url https://www.vulncheck.com/advisories/changedetection-io-through-0.60.6-ssrf-via-browser-step-goto-url	poc	yes	partial
CVE-2026-93435	7,5	redis-parser	Uncontrolled Recursion	through 3.0.0	https://github.com/NodeRedis/node-redis-parser https://github.com/NodeRedis/node-redis-parser/blob/701655430f5f7d9ca00892a02f7eefcbc1193a98/lib/parser.js#L204-L213 https://github.com/NodeRedis/node-redis-parser/blob/701655430f5f7d9ca00892a02f7eefcbc1193a98/lib/parser.js#L291-L306 https://github.com/redis/redis/issues/2108 https://www.vulncheck.com/advisories/redis-parser-through-3.0.0-denial-of-service-via-unbounded-recursion			
CVE-2026-93452	7,5	snappy-java	Out-of-bounds Write	through 1.1.10.8	https://github.com/xerial/snappy-java https://github.com/xerial/snappy-java/blob/v1.1.10.8/src/main/java/org/xerial/snappy/Snappy.java#L137 https://github.com/xerial/snappy-java/issues/732 https://www.vulncheck.com/advisories/snappy-java-through-1.1.10.8-buffer-overflow-in-snappy-compress			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-20222	7,4	Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software	Missing Release of Memory after Effective Lifetime	9.19.1; 9.19.1.5; 9.19.1.9; 9.19.1.12; 9.19.1.18; 9.20.1; 9.19.1.22; 9.20.1.5; 9.19.1.24; 9.20.2; 9.19.1.27; 9.20.2.10; 9.19.1.28; 9.20.2.21; 9.19.1.31; 9.20.2.22; 9.20.3; 9.23.1; 9.22.1.1; 9.20.3.4; 9.20.3.7; 9.19.1.37; 9.20.3.9; 9.19.1.38; 9.22.1.3; 9.20.3.10; 9.22.1.2; 9.20.3.13; 9.22.1.6; 9.22.2; 9.20.3.16; 9.19.1.42; 9.23.1.3; 9.20.3.20; 9.22.2.4; 9.23.1.7; 9.20.4; 9.22.2.9; 9.23.1.13; 9.20.4.7; 9.22.2.13; 9.20.4.10; 9.23.1.19; 9.22.2.14; 9.24.1; 9.23.1.22; 9.20.4.14; 9.22.2.20; 9.20.4.19; 9.23.1.26; 9.22.2.32; 9.22.3; 9.24.1.5; 9.20.4.22; 9.24.1.9; 9.20.4.28; 9.22.3.5; 9.23.1.195; 9.20.4.30; 9.24.1.155; 9.23.1.32; 9.24.1.11; 9.20.4.34; 9.20.4.235; 7.3.0; 7.3.1; 7.3.1.1; 7.4.0; 7.4.1; 7.4.1.1; 7.3.1.2; 7.6.0; 7.4.2; 7.4.2.1; 7.7.0; 7.4.2.2; 7.6.1; 7.4.2.3; 7.6.2; 7.7.10; 7.7.11; 7.6.2.1; 7.7.10.1; 7.4.2.4; 7.4.3; 7.6.4; 10.0.0; 7.4.4; 7.4.7	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-eigrp-dos-GOhNeiSj	none	no	partial
CVE-2026-78501	7,4	Improper neutralization of special elements used in a command ('command injection') in Microsoft; a command ('command injection') in Microsoft 365 Copilot's Business Chat	Improper Neutralization of Special Elements used in a Command ('Command Injection'); Improper Restriction of Communication Channel to Intended Endpoints		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78501			
CVE-2026-90997	7,4	Keycloak	Authentication Bypass by Capture-replay	26.7.0 prior to 26.7.4	https://access.redhat.com/security/cve/cve-2026-90997 https://github.com/keycloak/keycloak			
CVE-2026-91734	7,4	Core in Google Chrome on on Windows	Incorrect Authorization	prior to 153.0.8010.47	https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0541751186.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-2026-92913	7,4	AVideo through commit c3edcc274c389816d434acadac07ee78eaf330c1	Use of Insufficiently Random Values	c3edcc274c389816d434acadac07ee78eaf330c1 and earlier	https://github.com/WWBN/AVideo/security/advisories/GHSA-v65f-hc7x-wj62 https://www.vulncheck.com/advisories/avideo-weak-prng-activation-code-authentication-bypass	poc	no	total
CVE-2026-76154	7,3	the Geomap panel's MapLibre base layer	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12.3.0; 12.4.0 through 12.4.10; 13.0.0 through 13.0.8; 13.1.0 through 13.1.5; 13.2.0 through 13.2.1	https://grafana.com/security/security-advisories/cve-2026-76154			
CVE-2026-92915	7,3	WWBN AVideo through commit e01e41ecc (no patched version available)	Allocation of Resources Without Limits or Throttling	29.0 and earlier	https://github.com/WWBN/AVideo/security/advisories/GHSA-rq4h-fcmm-8w26 https://www.vulncheck.com/advisories/wwbn-avideo-userverifyemail-php-unauthenticated-access-control	poc	yes	partial
CVE-2026-76424	7,2	the REST API of Cisco ISE	Relative Path Traversal	3.1.0; 3.1.0 p1; 3.1.0 p3; 3.1.0 p2; 3.2.0; 3.1.0 p4; 3.1.0 p5; 3.2.0 p1; 3.1.0 p6; 3.2.0 p2; 3.1.0 p7; 3.3.0; 3.2.0 p3; 3.2.0 p4; 3.1.0 p8; 3.2.0 p5; 3.2.0 p6; 3.1.0 p9; 3.3 Patch 2; 3.3 Patch 1; 3.3 Patch 3; 3.4.0; 3.2.0 p7; 3.3 Patch 4; 3.4 Patch 1; 3.1.0 p10; 3.3 Patch 5; 3.3 Patch 6; 3.4 Patch 2; 3.3 Patch 7; 3.4 Patch 3; 3.5.0; 3.4 Patch 4; 3.3 Patch 8; 3.2 Patch 8; 3.5 Patch 1; 3.3 Patch 9; 3.2 Patch 9; 3.4 Patch 5; 3.5 Patch 3; 3.5 Patch 2; 3.3 Patch 10; 3.3 Patch 11; 3.4 Patch 6; 3.2 Patch 10; 3.1.0 p72; 3.1.0 p11; 3.3 Patch 12	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-hrP9IQSQ	none	no	total
CVE-2026-52851	7,1	Traccar	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Prior to 6.14.0	https://github.com/traccar/traccar/commit/cd0dbaf5df806139f508cbafaba20b34e62b499e https://github.com/traccar/traccar/releases/tag/v6.14.0 https://github.com/traccar/traccar/security/advisories/GHSA-jx5h-fxhc-cc9w	poc	no	partial
CVE-2026-91014	7,1	The Realtyna Organic IDX plugin + WPL Real Estate WordPress plugin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	before 5.4.2	https://wpscan.com/vulnerability/a57a9fbd-6f77-463f-a9fa-79503c12a49c/	none	no	partial

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-92602	7,1	TDuck survey form	Server-Side Request Forgery (SSRF)	through version 5.3	https://github.com/TDuckCloud/tduck-survey-form https://github.com/TDuckCloud/tduck-survey-form/blob/9ad4e2dc75cdf5eacc8be0c73f0d4db3c265d43/tduck-webhook/src/main/java/com/tduck/cloud/webhook/controller/WebhookConfigController.java#L43-L47 https://github.com/TDuckCloud/tduck-survey-form/blob/9ad4e2dc75cdf5eacc8be0c73f0d4db3c265d43/tduck-webhook/src/main/java/com/tduck/cloud/webhook/service/sender/WebhookSenderService.java#L84-L100 https://github.com/TDuckCloud/tduck-survey-form/issues/40 https://www.vulncheck.com/advisories/tduck-survey-form-through-5.3-server-side-request-forgery-via-unvalidated-webhook-url			
CVE-2026-92925	7,1	Redis community	Out-of-bounds Read		https://access.redhat.com/security/cve/CVE-2026-92925 https://bugzilla.redhat.com/show_bug.cgi?id=2535971 https://github.com/redis/redis/commit/37894faeea11e2db28b9fc2af378a762d2c36523 https://github.com/redis/redis/pull/15263 https://github.com/redis/redis/releases/tag/8.10.0	none	no	partial
CVE-2026-93014	7,1	RosarioSIS versions	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	versions before 12.9	https://gist.github.com/kazisabu/68bd095bc05b2341db318a063e05e644 https://gitlab.com/francoisjacquet/rosariosis https://gitlab.com/francoisjacquet/rosariosis/-/commit/701f9c07330157181362927a40d4f8dcc8094d90 https://www.vulncheck.com/advisories/rosariosis-before-12.9-path-traversal-in-file-deletion-via-filename-parameter	poc	no	partial
CVE-2026-93485	7,1	Automattic WordPress core	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7; before 7.1.1; 7.0 through 7.0.4; 6.9 through 6.9.7; 6.8 through 6.8.8; 6.7 through 6.7.7; 6.6 through 6.6.7; 6.5 through 6.5.10; 6.4 through 6.4.10; 6.3 through 6.3.10; 6.2 through 6.2.11; 6.1 through 6.1.12; 6.0 through 6.0.14; 5.9 through 5.9.16; 5.8 through 5.8.15; 5.7 through 5.7.17; 5.6 through 5.6.19; 5.5 through 5.5.20; 5.4 through 5.4.21; 5.3 through 5.3.23; 5.2 through 5.2.26; 5.1 through 5.1.24; 5.0 through 5.0.27; 4.9 through 4.9.31; 4.8 through 4.8.30; 4.7 through 4.7.35.	https://patchstack.com/database/wordpress/wordpress/wordpress/vulnerability/wordpress-wordpress-wordpress-7-1-cross-site-scripting-xss-vulnerability? s_id=cve https://wordpress.org/news/2026/09/wordpress-7-1-1-maintenance-and-security-release/			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-68904	7,0	node-opcua	Uncontrolled Resource Consumption	>= 2.0.0, < 2.170.0	https://github.com/node-opcua/node-opcua/commit/1959cbb8946b386d2e24a1cce05b7148099d36e7 https://github.com/node-opcua/node-opcua/commit/481664fa6ba8204737c5a92797ff68c3ae780c1c https://github.com/node-opcua/node-opcua/commit/4d59197e2dbd82791d7f36dad7da178715e0c27a https://github.com/node-opcua/node-opcua/commit/dc406fd2d364aa69dd173be21ed32a7ff425017a https://github.com/node-opcua/node-opcua/pull/1497 https://github.com/node-opcua/node-opcua/releases/tag/v2.170.0	none	no	partial

CISA/CERT-EU Alerts & Advisories

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

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds Two Known Exploited Vulnerabilities to Catalog CISA	CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog , based on evidence of active exploitation.	https://cisa.gov/news-events/alerts/2026/09/16/cisa-adds-two-known-exploited-vulnerabilities-catalog

News

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

Σύντομη περιγραφή / Τίτλος	URL
MIND Secures \$72 Million for AI-Powered DLP	https://securityweek.com/mind-secures-72-million-for-ai-powered-dlp
AI Agent Breaches Spanish Organization, Modifies Personal Data	https://darkreading.com/cyberattacks-data-breaches/ai-agent-breaches-spanish-organization-personal-data
OpenAI details more cases of AI agents taking unauthorized actions	https://bleepingcomputer.com/news/security/openai-details-more-cases-of-ai-agents-taking-unauthorized-actions
Cyberattacks on Two Oil Tankers Prompt Coast Guard, FBI to Board Vessels	https://securityweek.com/cyberattacks-on-two-oil-tankers-prompt-coast-guard-fbi-to-board-vessels

Σύντομη περιγραφή / Τίτλος	URL
OpenAI Models Searched for Leaked API Keys and Uploaded Files Without Permission	https://cybersecuritynews.com/openai-models-api-key-leaks
FBI Takes Down NightmareStresser DDoS Service Used in Hundreds of Thousands of Attacks	https://cybersecuritynews.com/nightmarestresser-ddos-service
OpenAI Says Its Models Searched GitHub for Leaked API Keys During Training	https://securityweek.com/openai-says-its-models-hunted-github-for-leaked-api-keys-during-training
CISA Wants Defenders to Deploy Fake Credentials and Systems to Catch Hackers	https://cybersecuritynews.com/cisa-fake-credentials-catch-hackers
CISA Urges Critical Infrastructure to Plant Decoys Inside Networks	https://infosecurity-magazine.com/news/cisa-critical-infrastructure-cyber
Windows 11 24H2 Home and Pro reach end of support in October	https://bleepingcomputer.com/news/microsoft/windows-11-24h2-home-and-pro-reach-end-of-support-in-october
Comp AI Raises \$34 Million for AI-Native Compliance and Security	https://securityweek.com/comp-ai-raises-34-million-for-ai-native-compliance-and-security
Cyber Essentials Has Record Year but Takeup Remains Low	https://infosecurity-magazine.com/news/cyber-essentials-has-record-year
North Korean IT Workers Use AI and Remote Desktop Tools to Fake Technical Interviews	https://cybersecuritynews.com/north-korean-it-workers-2
Can You Prove a New CVE Is Exploitable Before Attackers Do? Learn How in This Webinar	https://thehackernews.com/2026/09/can-you-prove-new-cve-is-exploitable.html
US takes down NightmareStresser DDoS-for-hire platform	https://bleepingcomputer.com/news/security/fbi-seizes-nightmarestresser-service-linked-to-thousands-of-ddos-attacks
AWS Says Some Cloud Data Cannot Be Recovered After Data Centers Suffer War Damage	https://cybersecuritynews.com/aws-cloud-data-war-damage
OpenAI Reveals Six Model Incidents Involving Hidden Failures and Unauthorized Uploads	https://thehackernews.com/2026/09/openai-reveals-six-model-incidents.html
Privacy Policy	https://cybersecuritynews.com/privacy-policy-2
AI Agent Carries Out Multi-Stage Data Theft Attack	https://infosecurity-magazine.com/news/ai-agent-carries-out-multistage
Microsoft shares workaround for Windows domain login issues	https://bleepingcomputer.com/news/microsoft/microsoft-releases-workaround-for-windows-domain-login-authentication-issues

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
Revolut Data Breach: 5 Months, 680 High-Profile Accounts, \$3M Ransom	https://securityweek.com/revolut-data-breach-5-months-680-high-profile-accounts-3m-ransom
Hacked Thai College Website Abused to Redirect Google Searchers to Illegal Online Casino	https://cybersecuritynews.com/hacked-thai-college-website-abused-to-redirect-google-searchers-to-illegal-online-casino
Gyazo Breach Exposes 23.62 Million User Records and 490 Million Image Metadata Records	https://thehackernews.com/2026/09/gyazo-breach-exposes-2362-million-user.html
Spain's data agency gets first report of AI-powered data breach	https://bleepingcomputer.com/news/security/spains-data-agency-gets-first-report-of-ai-powered-data-breach

Vulnerabilities / Flaws / Zero-day

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

Σύντομη περιγραφή / Τίτλος	URL
Check Point, Kaspersky, Tanium Patch Product Vulnerabilities	https://securityweek.com/check-point-kaspersky-tanium-patch-product-vulnerabilities
Researchers Use Claude Opus 5 to Hack OpenAI Forum and Reach Internal Repositories	https://cybersecuritynews.com/opus-5-to-help-exploit-openai-flaws
Steam Windows 0-Day Vulnerability Allows Users to Silently Escalate to Full SYSTEM Privileges	https://cybersecuritynews.com/steam-windows-0-day-vulnerability
Critical Check Point Management Flaw Lets Unauthenticated Attackers Run Code as Root	https://thehackernews.com/2026/09/critical-check-point-management-server.html
ThreatsDay: Self-Rewriting Agents, 800+ Flaws Patched, Insider SIM Swaps and 22 More New Stories	https://thehackernews.com/2026/09/threatsday-self-rewriting-agents-800.html
Critical Docker Sandboxes Flaw Lets Malicious Guest Code Read and Modify macOS Host Files	https://thehackernews.com/2026/09/critical-docker-sandboxes-flaw-lets.html
BIND DNS Servers Hit by 14 Security Flaws Enabling Cache Poisoning and Remote Crashes	https://cybersecuritynews.com/bind-dns-servers-hit-by-14-security-flaws
CISA Retires Weekly Vulnerability Bulletin in Risk-Based Pivot	https://securityweek.com/cisa-retires-weekly-vulnerability-bulletin-in-risk-based-pivot
Critical Unbound DNSSEC Validator Flaw Could Allow RCE via a Malicious DNS Zone	https://thehackernews.com/2026/09/critical-unbound-dnssec-validator-flaw.html
Critical Docker Sandbox Vulnerabilities Enable Malicious Guests to Escape Isolated microVM Workspaces	https://cybersecuritynews.com/critical-docker-sandboxes-vulnerabilities
Cisco Warns of Active Exploitation of Critical ISE Flaw	https://infosecurity-magazine.com/news/cisco-active-exploitation-critical
Cisco Warns of Critical ISE 0-Day Vulnerability Exploited in Attacks	https://cybersecuritynews.com/cisco-warns-of-critical-ise-0-day-vulnerability-exploited
Hackers Allegedly Selling Fortinet FortiGate 1-Day Vulnerability on Underground Forums	https://cybersecuritynews.com/hackers-selling-fortinet-fortigate-1-day-vulnerability
Cisco warns of max severity ISE zero-day exploited in attacks	https://bleepingcomputer.com/news/security/cisco-warns-of-identity-service-engine-zero-day-exploited-in-attacks
Cisco Warns of New Zero-Day ISE Auth Bypass (CVSS 10.0) Exploited in Active Attacks	https://thehackernews.com/2026/09/cisco-warns-of-new-zero-day-ise-auth.html
Active Exploitation Triggers Emergency Patch for Cisco ISE Zero-Day	https://securityweek.com/active-exploitation-triggers-emergency-patch-for-cisco-ise-zero-day
Check Point Vulnerability Lets Remote Hackers Gain Root Access Without Authentication	https://cybersecuritynews.com/check-point-root-access-flaw
Attackers Exploit Issabel Framework Flaw Enabling Unauthenticated OS Command Execution	https://thehackernews.com/2026/09/attackers-exploit-issabel-framework.html
CISA Warns of Critical ScreenConnect Vulnerability Actively Exploited in Attacks	https://cybersecuritynews.com/screenconnect-vulnerability-exploited
Parallels Desktop Flaw Lets Non-Admin Mac Users Gain Root, but Intel Macs Can't Install Fix	https://thehackernews.com/2026/09/parallels-desktop-flaw-lets-non-admin.html

Patches / Updates / Fixes

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

Σύντομη περιγραφή / Τίτλος	URL
WordPress Urges Immediate Update After Fixing 11 Security Vulnerabilities	https://cybersecuritynews.com/wordpress-7-1-1-security-update
Microsoft fixes broken copy and paste for Excel 2016 users	https://bleepingcomputer.com/news/microsoft/microsoft-fixes-broken-copy-and-paste-for-excel-2016-users
ISC Patches 14 Vulnerabilities in BIND 9 Security Update	https://securityweek.com/isc-patches-14-vulnerabilities-in-bind-9-security-update
Cisco Fixes Dozens of Flaws Across FMC, ISE and Nexus Dashboard	https://securityweek.com/cisco-fixes-dozens-of-flaws-across-fmc-ise-and-nexus-dashboard
BIND 9 Update Fixes 14 Flaws, Including an Unauthenticated Crash Over DNS-over-HTTPS	https://thehackernews.com/2026/09/bind-9-update-fixes-14-flaws-including.html
Google Patches Pixel Modem Flaw Amid Signs of Limited Targeted Exploitation	https://thehackernews.com/2026/09/google-patches-pixel-modem-flaw-amid.html
Acronis Patches Exploited Vulnerability in cPanel Backup Plugin	https://securityweek.com/acronis-patches-exploited-vulnerability-in-cpanel-backup-plugin
Oracle Patches 800+ Vulnerabilities in September 2026 Security Update	https://securityweek.com/oracle-patches-800-vulnerabilities-in-september-2026-security-update

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
Hackers Poison Movie Torrents With MovieReaper Malware That Uses Solana for C2	https://cybersecuritynews.com/poison-movie-torrents
New RatHat Android malware uses AI to automate device control	https://bleepingcomputer.com/news/security/new-rathat-android-malware-uses-ai-to-automate-device-control
China's FamousSparrow APT Spies on US Politics in Latin America	https://darkreading.com/cyberattacks-data-breaches/china-famous-sparrow-spies-latin-america
Brevo supply-chain attack injected ClickFix scripts on customer sites	https://bleepingcomputer.com/news/security/brevo-supply-chain-attack-injected-clickfix-scripts-on-customer-sites
FamousSparrow Swaps SparrowDoor For New SparrowWocky Backdoor	https://infosecurity-magazine.com/news/famous-sparrow-sparrowocky-latin
New 'RatHat' Android Malware Leverages AI to Steal Financial Data	https://infosecurity-magazine.com/news/rathat-android-malware-ai-steal
Hackers Turn Telegram Into a Command Center for HEAVYGRAM Surveillance Malware	https://cybersecuritynews.com/heavygram-surveillance-malware

Σύντομη περιγραφή / Τίτλος	URL
Ransomware Attacks on Manufacturers Surge as Supply Chain Risk Grows	https://securityweek.com/ransomware-attacks-on-manufacturers-surge-as-supply-chain-risk-grows
FamousSparrow Exploits Public-Facing Exchange Servers to Deploy SparrowWocky Backdoor	https://cybersecuritynews.com/famoussparrow-exploits
Chinese hackers use SparrowWocky malware in govt espionage attacks	https://bleepingcomputer.com/news/security/chinese-hackers-use-sparrowocky-malware-in-govt-espionage-attacks
Iranian hackers use CHOSEN BRICK Windows malware to spy on targets	https://bleepingcomputer.com/news/security/iranian-hackers-use-chosen-brick-windows-malware-to-spy-on-targets
Malware bypasses browser checks to force install Chrome, Edge extensions	https://bleepingcomputer.com/news/security/malware-bypasses-browser-checks-to-force-install-chrome-edge-extensions
Three Threat Groups Target Russian Enterprises With Backdoors, Ransomware, and Wipers	https://thehackernews.com/2026/09/three-threat-groups-target-russian.html
PHP Webshell Campaign Targets WordPress Through WooCommerce Bug	https://infosecurity-magazine.com/news/woocommerce-wholesale-lead-capture
GhostCode Phishing Kit Bypasses Microsoft 365 MFA to Hijack Accounts in 78 Seconds	https://cybersecuritynews.com/ghostcode-phishing-kit

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
CISO's Expert Guide to Agentic Pentesting for Websites	https://thehackernews.com/2026/09/cisos-expert-guide-to-agentic.html

References

- [1]. Ο βαθμός επικινδυνότητας είναι σύμφωνα με την κλίμακα Common Vulnerability Scoring System (CVSSv3), <https://nvd.nist.gov/vuln-metrics/cvss>
- [2]. Τα CVEs αποτελέσματα που εμφανίζονται στην ενότητα 1 διαθέτουν CVSS v3.1 score ≥ 7.0 , αφορούν το διάστημα 16/09/2026–18/09/2026, και έχει γίνει μια επιλογή συστημάτων/υπηρεσιών ανάλογα με το πόσο διαδεδομένα είναι.

Annex – Websites with vendor specific vulnerabilities

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

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