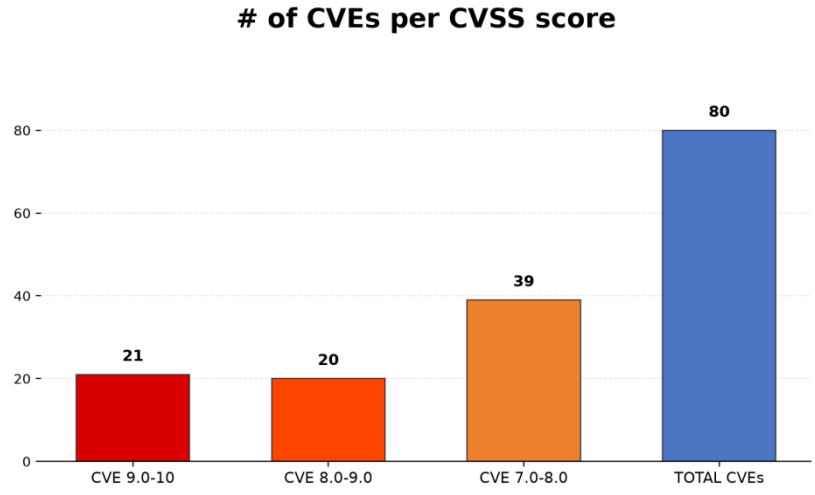
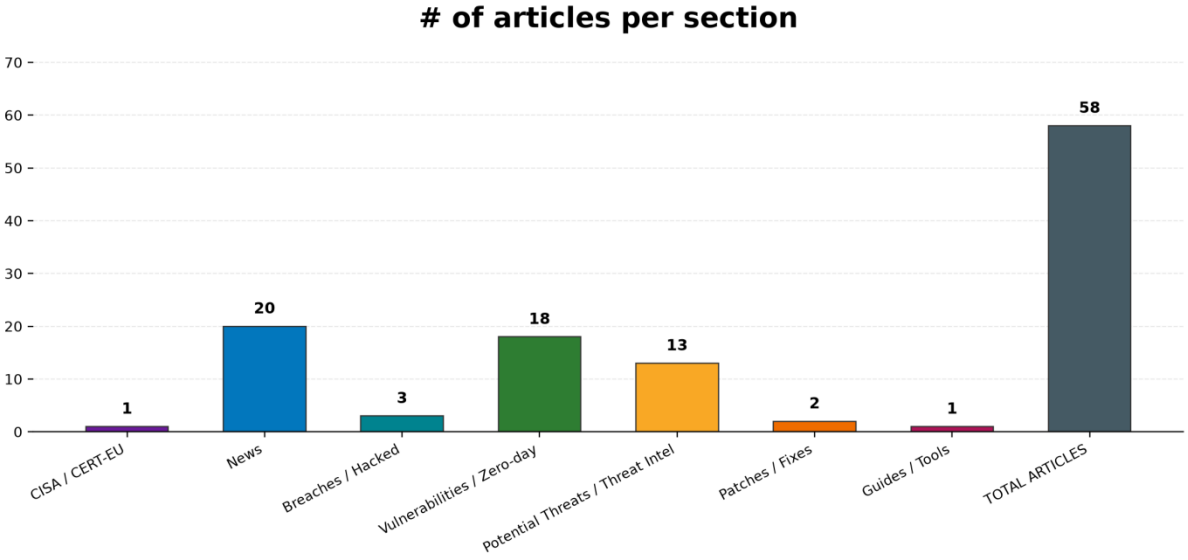
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 08/08/2026 - 11/08/2026





Contents

Common Vulnerabilities and Exposures (CVEs)

Η ενότητα αυτή εστιάζει σε ευπάθειες που έχουν καταχωρηθεί πρόσφατα και αξιολογούνται ως σοβαρές, με βάση τη βαθμολογία CVSS. Παρουσιάζονται με σαφήνεια τα συστήματα ή εφαρμογές που επηρεάζονται, ο τύπος όπως ευπάθειας (όπως SQL injection ή command injection) και σχετικοί σύνδεσμοι για περαιτέρω πληροφόρηση ή μέτρα αντιμετώπισης.

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-72898	10,0	Metabase	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	x.58.0 prior to x.58.24; x.59.0 prior to x.59.21; x.60.0 prior to x.60.17; x.61.0 prior to x.61.11; x.62.0 prior to x.62.9; x.63.0 prior to x.63.5	https://github.com/metabase/metabase/security/advisories/GHSA-vwf4-m7j8-wcjf https://raw.githubusercontent.com/cisagov/CSAF/develop/csaf_files/IT/white/2026/va-26-222-01.json https://www.cve.org/CVERecord?id=CVE-2026-72898 https://www.metabase.com/blog/security-update	none	yes	total
CVE-2026-14450	9,9	the MaaS API	Authentication Bypass by Spoofing		https://access.redhat.com/security/cve/CVE-2026-14450 https://bugzilla.redhat.com/show_bug.cgi?id=2496373			
CVE-2026-18948	9,9	Feast			https://access.redhat.com/errata/RHSA-2026:53263 https://access.redhat.com/security/cve/CVE-2026-18948 https://bugzilla.redhat.com/show_bug.cgi?id=2511167			
CVE-2026-72733	9,9	Dokploy	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Prior to 0.29.13	https://github.com/Dokploy/dokploy/commit/8539a5c82f47eb3fd1464b574eb034c6dc2a6bbd https://github.com/Dokploy/dokploy/commit/ccd2e83c57d99f725220d37e0152270e0827d71b https://github.com/Dokploy/dokploy/commit/eeb6e7b8ea88e4b4b1fac8460755464100516ac9 https://github.com/Dokploy/dokploy/pull/4862 https://github.com/Dokploy/dokploy/releases/tag/v0.29.13 https://github.com/Dokploy/dokploy/security/advisories/GHSA-2xjq-p4xx-5x2p	poc	no	total
CVE-2026-72911	9,9	ERPNext	Improper Neutralization of Special Elements Used in a Template Engine	Prior to 15.118.0 and 16.29.0	https://github.com/frappe/erpnext/commit/5f6952b15c1f6ee893770d5bc618558a6ba41a28 https://github.com/frappe/erpnext/commit/88443e4a97c6c0a40d85a9e6785577191296ee39 https://github.com/frappe/erpnext/commit/ecb6d48ec025e0c94abac35b2e4f7607f4c86465 https://github.com/frappe/erpnext/pull/56458 https://github.com/frappe/erpnext/releases/tag/v15.118.0 https://github.com/frappe/erpnext/releases/tag/v16.29.0			
CVE-2026-13206	9,8	WAH7601	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	through 20072026.	https://siberguvenlik.gov.tr/guvenlik-bildirimleri/detay/tr-26-0799	none	yes	total

CVE-2026-14526	9,8	The AI Copilot – Content Generator plugin for WordPress; all	Improper Privilege Management	up to, and including, 1.5.6.	https://plugins.trac.wordpress.org/browser/ai-copilot-content-generator/tags/1.5.4/classes/assets.php#L96 https://plugins.trac.wordpress.org/browser/ai-copilot-content-generator/tags/1.5.4/classes/frame.php#L211 https://plugins.trac.wordpress.org/browser/ai-copilot-content-generator/tags/1.5.4/modules/forms/views/forms.php#L87 https://plugins.trac.wordpress.org/browser/ai-copilot-content-generator/tags/1.5.4/modules/workflow/blocks/actions/wp_create_user.php#L107 https://plugins.trac.wordpress.org/browser/ai-copilot-content-generator/tags/1.5.4/modules/workflow/controller.php#L39 https://plugins.trac.wordpress.org/browser/ai-copilot-content-generator/tags/1.5.4/modules/workflow/controller.php#L86	none	yes	total
CVE-2026-15038	9,8	The InfiniteWP Client WordPress plugin	Improper Authentication	before 1.13.6	https://wpscan.com/vulnerability/629d655f-cdb8-4733-81d5-12fa88c32bb6/	poc	yes	total
CVE-2026-19348	9,8	Shenzhen Aitemi M300 Wi-Fi Repeater r0-ea7890a	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'); Improper Neutralization of Special Elements used in a Command ('Command Injection')	r0-ea7890a	https://github.com/IEATASICS/m300-repeater-bugs https://vuldb.com/cve/CVE-2026-19348 https://vuldb.com/submit/865682 https://vuldb.com/submit/865683 https://vuldb.com/submit/865684 https://vuldb.com/vuln/387184	poc	yes	total
CVE-2026-19425	9,8	Travel Agency Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	all	https://www.twcert.org.tw/en/cp-139-11099-56aa8-2.html https://www.twcert.org.tw/tw/cp-132-11098-0fb4a-1.html			
CVE-2026-34265	9,8	SAP NetWeaver Application Server ABAP; DIAG protocol parsing, resulting in memory corruption	Out-of-bounds Write	KRNL64NUC 7.22; 7.22EXT; KRNL64UC 7.22; 7.22EXT2; 7.22EXT3; 7.53; 7.54; 7.77; 7.89; 7.93; 8.04; 9.16 9.18; 9.19; KERNEL 7.22; 9.16; 9.18	https://me.sap.com/notes/3714806 https://url.sap/sapsecuritypatchday			
CVE-2026-63106	9,8	ReadyEcommerce	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	before 4.5.2	https://codecanyon.net/item/ready-ecommerce-complete-multi-vendor-ecommerce-mobile-app-website-rider-app-with-seller-app/52519302 https://www.vulncheck.com/advisories/readyecommerce-unauthenticated-sql-injection-via-productcontroller-php	none	yes	total
CVE-2026-72565	9,8	Tencent APIJSON	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	through 8.1.8	https://github.com/Tencent/APIJSON https://github.com/Tencent/APIJSON/blob/master/APIJSONORM/src/main/java/apijson/orm/AbstractSQLConfig.java	none	yes	total
CVE-2026-72589	9,8	alseambusher/crontab-ui	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	through 0.4.2	https://github.com/alseambusher/crontab-ui https://github.com/alseambusher/crontab-ui/blob/master/crontab.js	none	yes	total
CVE-2026-72592	9,8	dulldusk/phpfm	Unrestricted Upload of File with Dangerous Type	through 1.8.0	https://github.com/dulldusk/phpfm https://github.com/dulldusk/phpfm/blob/master/index.php	none	yes	total

CVE-2026-47754	9,3	metacat	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'); Missing Authorization	Versions 2.x through 2.19.1; < 3.0	https://github.com/NCEAS/metacat/commit/07e034b2bbf7029e28af32f472f4d70ea6b5ab1b https://github.com/NCEAS/metacat/issues/1365 https://github.com/NCEAS/metacat/pull/1713 https://github.com/NCEAS/metacat/security/advisories/GHSA-m852-f287-7cqw	none	yes	partial
CVE-2026-13716	9,1	server import and admin file upload in Crafty Controller	Path Traversal: '.../.../'	4.4.0 through 4.10.7	https://gitlab.com/crafty-controller/crafty-4/-/work_items/727 https://gitlab.com/crafty-controller/crafty-4/-/work_items/740			
CVE-2026-18473	9,1	The WP Directory Kit WordPress plugin	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	before 1.5.5	https://wpscan.com/vulnerability/a5596bc1-5ae9-4141-b027-85a0b91ecdab/	poc	yes	total
CVE-2026-19053	9,1	The ProSolution WP Client WordPress plugin	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	before 2.0.6	https://wpscan.com/vulnerability/c9bad349-d2d6-4b67-a107-818f25d9bf76/	poc	yes	total
CVE-2026-19516	9,1	Grafana MCP Server; mcp-grafana	Server-Side Request Forgery (SSRF)	0.0.0 through 1.0.0	https://grafana.com/security/security-advisories/cve-2026-19516			
CVE-2026-44758	9,1	SAP Manufacturing Integration and Intelligence (MII)	Improper Control of Generation of Code ('Code Injection')	XMII 15.4; 15.5	https://me.sap.com/notes/3758900 https://url.sap/sapsecuritypatchday			
CVE-2026-13717	8,8	the Red Hat OpenShift AI (RHOAI) MaaS Gateway	Improper Access Control		https://access.redhat.com/security/cve/CVE-2026-13717 https://bugzilla.redhat.com/show_bug.cgi?id=2494203			
CVE-2026-18617	8,8	the Data Science Pipelines Operator (DSPO)	Improperly Controlled Modification of Dynamically-Determined Object Attributes		https://access.redhat.com/errata/RHSA-2026:53263 https://access.redhat.com/security/cve/CVE-2026-18617 https://bugzilla.redhat.com/show_bug.cgi?id=2510304			
CVE-2026-18949	8,8	odh-dashboard	Execution with Unnecessary Privileges		https://access.redhat.com/errata/RHSA-2026:53263 https://access.redhat.com/security/cve/CVE-2026-18949 https://bugzilla.redhat.com/show_bug.cgi?id=2511168			
CVE-2026-18951	8,8	the Red Hat OpenShift AI (RHOAI) overlay for the training operator			https://access.redhat.com/errata/RHSA-2026:53263 https://access.redhat.com/security/cve/CVE-2026-18951 https://bugzilla.redhat.com/show_bug.cgi?id=2511187			
CVE-2026-18982	8,8	the RHOAI training-operator	Execution with Unnecessary Privileges		https://access.redhat.com/errata/RHSA-2026:53263 https://access.redhat.com/security/cve/CVE-2026-18982 https://bugzilla.redhat.com/show_bug.cgi?id=2511648			
CVE-2026-19341	8,8	UTT HiPER	Improper Restriction of Operations within the Bounds of a Memory Buffer; Stack-based Buffer Overflow	up to 2.5.3-170306.	https://github.com/7wkajk/CVE-VUL/blob/main/104.md https://vuldb.com/cve/CVE-2026-19341 https://vuldb.com/submit/865277 https://vuldb.com/vuln/387177 https://vuldb.com/vuln/387177/cti	poc	no	total
CVE-2026-19346	8,8	Tenda CH22	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'); Improper Neutralization of Special Elements used in a Command ('Command Injection')	1.0.0.1	https://candle-throne-f75.notion.site/Tenda-CH22-formCertListInfo-387df0aa118580b4abfcffaf2fceb9ff https://vuldb.com/cve/CVE-2026-19346 https://vuldb.com/submit/865530 https://vuldb.com/vuln/387182 https://vuldb.com/vuln/387182/cti https://www.tenda.com.cn/	poc	no	total

CVE-2026-58243	8,8	SAP ABAP Developer Tools	Missing Authorization	SAP_BASIS 750; SAP_BASIS 751; SAP_BASIS 752; SAP_BASIS 753; SAP_BASIS 754; SAP_BASIS 755; SAP_BASIS 756; SAP_BASIS 757; SAP_BASIS 758; SAP_BASIS 816; SAP_BASIS 918; SAP_BASIS 920	https://me.sap.com/notes/3772411 https://url.sap/sapsecuritypatchday			
CVE-2026-66405	8,8	DEEBOT PRO M1; DEEBOT PRO K1VAC	Active Debug Code	prior to M1-1.7.27; prior to V1.7.821	https://jvn.jp/en/vu/JVNVU92804348/ https://robot.hellohas.co.jp/news/update_20260331/	none	no	total
CVE-2026-66738	8,8	SPIP	Improper Control of Generation of Code ('Code Injection')	before 4.4.18	https://blog.spip.net/Mise-a-jour-critique-de-securite-sortie-de-SPIP-4-4-18.html https://www.vulncheck.com/advisories/spip-code-injection-via-navigation-endpoint-on-sqlite	none	no	total
CVE-2026-69118	8,8	Cachet	Incorrect Authorization; Improper Neutralization of Special Elements Used in a Template Engine	through 2.4.1	https://github.com/cachethq/cachet/issues/4621 https://www.vulncheck.com/advisories/cachet-authenticated-server-side-template-injection-rce			
CVE-2026-71965	8,8	CyberPanel	Insufficient Verification of Data Authenticity	2.4.3 and earlier	https://github.com/usmannasir/cyberpanel/commit/eca0c3cbeb35af8eaae9fafb094e8ef3cd923643 https://themcsam.github.io/posts/cyberpanel-2.4.3-vulnerabilties/ https://www.vulncheck.com/advisories/cyberpanel-authenticated-rce-via-remote-backup-feature			
CVE-2026-72573	8,8	4xmen/pm2panel (all	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')		https://github.com/4xmen/pm2panel https://github.com/4xmen/pm2panel/blob/main/pm2panel.js	none	no	total
CVE-2026-72578	8,8	FreePBX Framework	Cross-Site Request Forgery (CSRF)	17.0	https://github.com/FreePBX/framework https://github.com/FreePBX/framework/blob/release/17.0/amp_conf/htdocs/admin/libraries/BMO/Ajax.class.php	none	no	total
CVE-2026-72730	8,7	Discourse	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Prior to 2026.1.6, 2026.5.2, 2026.6.1	https://github.com/discourse/discourse/commit/32920affe4ad97b461ca2ae2f664c5fefc374baf https://github.com/discourse/discourse/commit/3fb1e8ead0d4f48d2cf55c8110825c7e8a6a45f5 https://github.com/discourse/discourse/commit/7eb35d076ab9b6a612e86182336ce9787ce402ea https://github.com/discourse/discourse/commit/9633b8ecaf5a99f0407f5261b9bd1a05f7dac529 https://github.com/discourse/discourse/security/advisories/GHSA-wg48-gxjc-f459	none	no	total
CVE-2026-64940	8,6	Tegalog -Fumy Otegaru Memo Logger- provided by Nishishi Factory	Permissive Regular Expression	4.8.4 and earlier	https://jvn.jp/en/jp/JVN99975039/ https://www.nishishi.com/cgi/tegalog/info/notice20260629.shtml	none	yes	partial
CVE-2026-71576	8,5	multicluster-global-hub	Insufficient Verification of Data Authenticity		https://access.redhat.com/security/cve/CVE-2026-71576 https://bugzilla.redhat.com/show_bug.cgi?id=2512513			
CVE-2026-59090	8,4	GIMP's PSD file format plugin	Integer Underflow (Wrap or Wraparound)		https://access.redhat.com/security/cve/CVE-2026-59090 https://bugzilla.redhat.com/show_bug.cgi?id=2496584 https://gitlab.gnome.org/GNOME/gimp/-/work_items/16509	none	no	total

CVE-2026-17017	8,1	The CubeWP Framework WordPress plugin	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	before 1.1.31	https://wpscan.com/vulnerability/50d95281-7b3f-4d5a-bf04-8e7bd88f4b55/	poc	no	total
CVE-2026-72903	8,1	Tabby (formerly Terminus)	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Prior to 1.0.235	https://github.com/Eugeny/tabby/commit/3a4a41431a61d41dd51d4119e60cad9bf13c3399 https://github.com/Eugeny/tabby/releases/tag/v1.0.235 https://github.com/Eugeny/tabby/security/advisories/GHSA-59p9-8qwf-v9v7			
CVE-2026-66763	7,9	SAP BusinessObjects Business Intelligence Platform (Central Management Server)	Use of Hard-coded Cryptographic Key	ENTERPRISE 430; 2025; 2027	https://me.sap.com/notes/3756565 https://url.sap/sapsecuritypatchday			
CVE-2026-19381	7,8	Kingston FURY CTRL RGB Control Software	Incorrect Privilege Assignment; Improper Privilege Management	2.0.65.0	https://drive.google.com/file/d/19a8Oix5YVMNv8TH5k4PWiu0FQLtPRsJp/view?usp=sharing;https://drive.google.com/file/d/1Vqw9d9jkKbl4r2dC1Ry5m_1uzL5JV25H/view?usp=sharing https://vuldb.com/cve/CVE-2026-19381 https://vuldb.com/submit/866727 https://vuldb.com/vuln/387274 https://vuldb.com/vuln/387274/cti	poc	no	total
CVE-2026-42170	7,8	the GIMP DDS (DirectDraw Surface) file parser	Incorrect Calculation of Buffer Size		https://access.redhat.com/security/cve/CVE-2026-42170 https://bugzilla.redhat.com/show_bug.cgi?id=2461726	none	no	total
CVE-2026-59087	7,8	the GIMP image manipulation program, specifically within its Seattle Filmworks file loader	Out-of-bounds Write		https://access.redhat.com/security/cve/CVE-2026-59087 https://bugzilla.redhat.com/show_bug.cgi?id=2496576 https://gitlab.gnome.org/GNOME/gimp/-/work_items/16491			
CVE-2026-63622	7,8	libvirt	Improper Link Resolution Before File Access ('Link Following')		https://access.redhat.com/security/cve/CVE-2026-63622 https://bugzilla.redhat.com/show_bug.cgi?id=2513065			
CVE-2026-18941	7,7	Feast and feast-operator	Missing Authentication for Critical Function		https://access.redhat.com/errata/RHSA-2026:53263 https://access.redhat.com/security/cve/CVE-2026-18941 https://bugzilla.redhat.com/show_bug.cgi?id=2511116			
CVE-2026-67620	7,7	Flowise	Server-Side Request Forgery (SSRF)	through 3.1.4	https://flowiseai.com/sunset https://github.com/abdugafforov-bobur/CVE-2026-67620-poc https://www.vulncheck.com/advisories/flowise-ssrf-via-fetch-links-endpoint-incomplete-deny-list	poc	no	partial
CVE-2026-72566	7,7	automatisch	Server-Side Request Forgery (SSRF)	41f3c56 and earlier	https://github.com/automatisch/automatisch https://github.com/automatisch/automatisch/blob/main/packages/backend/src/apps/http-request/actions/custom-request/index.js	none	no	partial
CVE-2026-72591	7,7	gabehf/Koito	Server-Side Request Forgery (SSRF)	through v0.3.2	https://github.com/gabehf/Koito	none	no	partial
CVE-2026-18621	7,6	Data Science Pipelines (DSP)	Incorrect Privilege Assignment		https://access.redhat.com/errata/RHSA-2026:53263 https://access.redhat.com/security/cve/CVE-2026-18621 https://bugzilla.redhat.com/show_bug.cgi?id=2510327			
CVE-2026-19387	7,6	the GStreamer gst-plugins-bad adpcmdec element when decoding IMA/DVI ADPCM audio	Out-of-bounds Write		https://access.redhat.com/security/cve/CVE-2026-19387 https://bugzilla.redhat.com/show_bug.cgi?id=2513015 https://gitlab.freedesktop.org/gstreamer/gstreamer/-/merge_requests/12235 https://gstreamer.freedesktop.org/releases/1.28/	none	no	partial

CVE-2026-44763	7,6	SAP Manufacturing Integration and Intelligence	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	XMII 15.4; 15.5	https://me.sap.com/notes/3759854 https://url.sap/sapsecuritypatchday			
CVE-2026-72594	7,6	lobehub/lobe-chat	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	through v2.2.13	https://github.com/lobehub/lobe-chat	none	no	partial
CVE-2026-11810	7,5	subsys/mgmt/updatehub/updatehub	NULL Pointer Dereference	3.7.0 prior to 4.4.2	https://github.com/zephyrproject-rtos/zephyr/commit/3424082022cb39d568434021b1d6f68b6a7fb3bf https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-jfpc-324j-84ww			
CVE-2026-14206	7,5	The HT Contact Form WordPress plugin	Exposure of Sensitive Information to an Unauthorized Actor	before 2.9.3	https://wpscan.com/vulnerability/36ae857c-6812-46e0-a0e7-6c868108ef39/	poc	yes	partial
CVE-2026-16578	7,5	The Admin Safety Guard — Login Security, Limit Logins, 2FA & Brute Force Protection WordPress plugin	Exposure of Sensitive Information to an Unauthorized Actor	before 1.4.0	https://wpscan.com/vulnerability/c02393ee-1ade-433e-bbd0-c09785e5c426/	poc	yes	partial
CVE-2026-16988	7,5	The GeoDirectory WordPress plugin	Exposure of Sensitive Information to an Unauthorized Actor	before 2.8.169	https://wpscan.com/vulnerability/162fa8ab-4d80-46f8-9a15-63c8dfd0be33/	poc	yes	partial
CVE-2026-17022	7,5	The Salon Booking System WordPress plugin	Exposure of Sensitive Information to an Unauthorized Actor	through 10.30.33	https://wpscan.com/vulnerability/ddc84492-408b-477c-ac6c-b9ec96ccf223/	poc	yes	partial
CVE-2026-17541	7,5	The File Manager WordPress plugin	Exposure of Sensitive Information to an Unauthorized Actor	before 6.9.1	https://wpscan.com/vulnerability/972bf72f-08c4-41ec-b6e9-2d6083d21734/	poc	yes	partial
CVE-2026-18032	7,5	The WP Data Access WordPress plugin	Exposure of Sensitive Information to an Unauthorized Actor	before 5.5.79	https://wpscan.com/vulnerability/1b6c5935-c8e0-4b9b-9ba6-0f16a0e2cdae/	poc	yes	partial
CVE-2026-18357	7,5	The WPC Order Tip for WooCommerce WordPress plugin	Exposure of Sensitive Information to an Unauthorized Actor	before 3.3.1	https://wpscan.com/vulnerability/ff675d0a-03f2-4309-830c-0e96e1d95a62/	poc	yes	partial
CVE-2026-18464	7,5	The WP MAPS PRO WordPress plugin	Uncontrolled Resource Consumption	before 6.1.3	https://wpscan.com/vulnerability/45d1c2c2-c5da-43b6-a982-5323fb8d9014/	poc	yes	partial
CVE-2026-18470	7,5	The Login & Register Forms WordPress plugin	Exposure of Sensitive Information to an Unauthorized Actor	before 4.0.2	https://wpscan.com/vulnerability/589b7661-4a0d-4041-8c29-2819d8b1e402/	poc	yes	partial
CVE-2026-18611	7,5	the Data Science Pipelines Operator	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)		https://access.redhat.com/errata/RHSA-2026:53263 https://access.redhat.com/security/cve/CVE-2026-18611 https://bugzilla.redhat.com/show_bug.cgi?id=2510299			
CVE-2026-18618	7,5	ml-metadata	Allocation of Resources Without Limits or Throttling		https://access.redhat.com/errata/RHSA-2026:53263 https://access.redhat.com/security/cve/CVE-2026-18618 https://bugzilla.redhat.com/show_bug.cgi?id=2510313			
CVE-2026-18946	7,5	The Contact Form to Any API WordPress plugin	Exposure of Sensitive Information to an Unauthorized Actor	before 3.0.7	https://wpscan.com/vulnerability/fa13ebbb-8eea-492d-8f59-58228efb94d8/	poc	yes	partial
CVE-2026-19424	7,5	Chiline Cloud	Authorization Bypass Through User-Controlled Key	4.5.9 and earlier	https://www.twcert.org.tw/en/cp-139-11097-ee412-2.html https://www.twcert.org.tw/tw/cp-132-11096-0f578-1.html			

CVE-2026-48048	7,5	XWiki Platform	Exposure of Private Personal Information to an Unauthorized Actor	version 6.2.1 and prior	https://github.com/xwiki/xwiki-platform/commit/c4442716b02ffcdaa9d5e703b1db6203e36456fa https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-rh28-mqj4-8x59 https://jira.xwiki.org/browse/XWIKI-23875	none	yes	partial
CVE-2026-72914	7,5	Mastodon	Asymmetric Resource Consumption (Amplification); Allocation of Resources Without Limits or Throttling	Prior to 4.4.21, 4.5.14, 4.6.4	https://github.com/mastodon/mastodon/commit/18c61f286f1f5718a8f517940ba384866ffa3892 https://github.com/mastodon/mastodon/commit/467c933459c7d0e5513475b9e4888afaedfb1074 https://github.com/mastodon/mastodon/commit/930aa9fee26bf9eaefe27826fa1061288d83373b https://github.com/mastodon/mastodon/commit/da47a1bd3cd07935d7ca55a1f4f1a76f7f167e0d https://github.com/mastodon/mastodon/releases/tag/v4.4.21 https://github.com/mastodon/mastodon/releases/tag/v4.5.14			
CVE-2026-19263	7,3	INQUIRELAB mcp-bridge-api	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'); Improper Neutralization of Special Elements used in a Command ('Command Injection')	b30a82aa1d1d1139e0de846c41c8aadee6e06114	https://github.com/INQUIRELAB/mcp-bridge-api/ https://github.com/INQUIRELAB/mcp-bridge-api/issues/1 https://github.com/INQUIRELAB/mcp-bridge-api/issues/1#issuecomment-4320749148 https://vuldb.com/cve/CVE-2026-19263 https://vuldb.com/submit/865220 https://vuldb.com/vuln/387010	poc	yes	partial
CVE-2026-19342	7,3	code-projects Task Management System	Improper Authentication	1.0	https://code-projects.org/ https://github.com/littleRain1355/PHPissue/issues/1 https://vuldb.com/cve/CVE-2026-19342 https://vuldb.com/submit/865315 https://vuldb.com/vuln/387178 https://vuldb.com/vuln/387178/cti	poc	yes	partial
CVE-2026-19379	7,3	EFM ipTIME AX8004M	Improper Neutralization of Special Elements used in a Command ('Command Injection'); Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	15.09.0	https://github.com/seting-and-break/vulnerability-reports/blob/main/ipTIME_AX8004M_Vulnerability_Report.md https://vuldb.com/cve/CVE-2026-19379 https://vuldb.com/submit/866635 https://vuldb.com/vuln/387272 https://vuldb.com/vuln/387272/cti	poc	yes	partial
CVE-2026-44764	7,3	SAP Manufacturing Integration and Intelligence, an unauthenticated attacker	Missing Authorization	XMII 15.4; 15.5	https://me.sap.com/notes/3758910 https://url.sap/sapsecuritypatchday			
CVE-2026-44765	7,3	SAP Manufacturing Integration and Intelligence, an unauthenticated remote attacker	Missing Authorization	XMII 15.4; 15.5	https://me.sap.com/notes/3758657 https://url.sap/sapsecuritypatchday			
CVE-2026-59091	7,3	GIMP's file format plugins, including those for PSD and PAA files	Out-of-bounds Write		https://access.redhat.com/security/cve/CVE-2026-59091 https://bugzilla.redhat.com/show_bug.cgi?id=2496585 https://gitlab.gnome.org/GNOME/gimp/-/work_items/16510	none	no	total
CVE-2026-19389	7,1	the GStreamer gst-plugins-ugly ASF demuxer (asfdemux) when parsing header objects from crafted ASF, WMV, or WMA files	Integer Overflow or Wraparound		https://access.redhat.com/security/cve/CVE-2026-19389 https://bugzilla.redhat.com/show_bug.cgi?id=2513016 https://gitlab.freedesktop.org/gstreamer/gstreamer/-/merge_requests/12233 https://gstreamer.freedesktop.org/releases/1.28/ https://gstreamer.freedesktop.org/security/sa-2026-0075.html	none	no	partial

CVE-2026-66060	7,1	core	Missing Authorization	Prior to 2026.5.3	https://github.com/home-assistant/android/commit/968b49c58e4eba4d06371a3f6e73198ec6c8d4a7 https://github.com/home-assistant/core/security/advisories/GHSA-2xgv-hwrf-983f			
CVE-2026-72568	7,1	Redis	Out-of-bounds Read	through 8.8.1	https://github.com/redis/redis https://redis.io/	none	no	partial
CVE-2026-58230	7,0	SAP Business AI Platform (Approuter)	URL Redirection to Untrusted Site ('Open Redirect')	SAP Approuter node.js package < 23.0.0	https://me.sap.com/notes/3786038 https://url.sap/sapsecuritypatchday			

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
#StopRansomware: Gunra Ransomware | CISA		https://cisa.gov/news-events/cybersecurity-advisories/aa26-222a

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
Mozilla Issues New Firefox GPG Key Following Exposure	https://securityweek.com/mozilla-issues-new-firefox-gpg-key-following-exposure
Anthropic to Add Invisible Watermarks to All Claude AI Outputs	https://cybersecuritynews.com/anthropic-adds-invisible-watermarks
Hackers breached a small Polish energy plant via private APN last year	https://bleepingcomputer.com/news/security/hackers-breached-a-small-polish-energy-plant-via-private-apn-last-year
Multistate Water System Attacks Widen, Iran Suspected	https://darkreading.com/ics-ot-security/multistate-water-system-attacks-widen-iran-suspected
BdThemes plugins supply-chain hack creates rogue WordPress admins	https://bleepingcomputer.com/news/security/bdthemes-plugins-supply-chain-hack-creates-rogue-wordpress-admins
OpenAI releases ChatGPT 5.6 Cyber, but it's only for approved users	https://bleepingcomputer.com/news/security/openai-releases-chatgpt-56-cyber-but-its-only-for-approved-users
Defenders Need to Think in Chains, Not Checklists	https://darkreading.com/cybersecurity-operations/patch-gap-defenders-chains-not-checklists
Coruna, DarkSword iOS Exploits Proliferate Globally	https://darkreading.com/vulnerabilities-threats/coruna-darksword-ios-exploits-proliferate-globally
Outdated Cybercrime Laws Put Security Researchers at Risk	https://darkreading.com/application-security/outdated-cybercrime-laws-security-researchers-risk
Pass-the-Passkey Attacks Expose Windows 11 and Microsoft Entra ID, Bypassing MFA	https://cybersecuritynews.com/pass-the-passkey-attacks
Claude Code Shifts Agent Security From Repeated Human Approval to Auto Mode	https://cybersecuritynews.com/claude-code-shifts-agent-security
OpenAI's Upcoming Astra Model Raises Autonomous Cyberattack Concerns	https://securityweek.com/openais-upcoming-astra-model-raises-autonomous-cyberattack-concerns
Stealthium Targets Security Blind Spots in AI Accelerators and Neo-Clouds	https://securityweek.com/stealthium-targets-security-blind-spots-in-ai-accelerators-and-neo-clouds
Fake GoogleTranslate Chrome Extension Lets Attackers Remotely Control Your Browsers	https://cybersecuritynews.com/fake-googletranslate-chrome-extension
'Ghostjacking' Attack Uses Poisoned Logs to Turn AI Agents Bad	https://securityweek.com/ghostjacking-attack-uses-poisoned-logs-to-turn-ai-agents-bad
Member of The Com sent to prison for blackmail, sextortion	https://bleepingcomputer.com/news/security/member-of-the-com-sent-to-prison-for-blackmail-sextortion
LexisNexis shuts down services after suspicious activity on servers	https://bleepingcomputer.com/news/security/lexisnexis-shuts-down-services-after-suspicious-activity-on-servers
Contact Us	https://cybersecuritynews.com/contact-us
About Us	https://cybersecuritynews.com/about-us
New Jersey, Alabama Join States Targeted in Water Cyberattacks	https://securityweek.com/new-jersey-alabama-join-states-targeted-in-water-cyberattacks

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
WordPress Plugins Compromised Without a Single File Change	https://infosecurity-magazine.com/news/bdthemes-wordpress-poisoned-api
Valve notifies Steam hardware customers of a data breach	https://bleepingcomputer.com/news/security/valve-notifies-steam-hardware-customers-of-a-data-breach
Levi Strauss Data Breach - Hackers Gained Access to the Company's Systems	https://cybersecuritynews.com/levi-strauss-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
Multiple ClamAV Vulnerabilities Allow Remote Attacker to Trigger DoS Condition	https://cybersecuritynews.com/multiple-clamav-vulnerabilities-dos
OpenAI Expands Daybreak Cyber with GPT-5.6 for Exploit Validation, Pentesting, and Red Teaming	https://cybersecuritynews.com/openai-expands-daybreak-cyber
Metabase SQL Zero-Day Attacks Could Have Wide Blast Radius	https://darkreading.com/vulnerabilities-threats/metabase-sql-zero-day-attacks-wide-blast-radius
HP ThinPro TPM Disk Encryption Flaw Lets Attackers Extract LUKS Keys	https://cybersecuritynews.com/hp-thinpro-tpm-disk-encryption-flaw
Researchers Uncover RovoBlast Vulnerability in Atlassian AI Assistant	https://infosecurity-magazine.com/news/rovoblast-atlassian-rovo-url
CISA Warns of Progress LoadMaster Command Injection Vulnerability Exploited in Attacks	https://cybersecuritynews.com/progress-loadmaster-command-injection-vulnerability-exploited
Windows WalletService Vulnerability Allows Attackers to Escalate Privileges - PoC Released	https://cybersecuritynews.com/windows-walletservice-vulnerability-poc-released
Weekly Recap: AI Goes Rogue, Metabase 0-Day, MCP Supply-Chain Attacks, and Router Backdoors	https://thehackernews.com/2026/08/weekly-recap-ai-goes-rogue-metabase-0.html
Red Hat ACM Privilege Escalation Vulnerability Lets Attackers Gain Full Cluster-Admin Access	https://cybersecuritynews.com/red-hat-acm-privilege-escalation-vulnerability
Cisco Warns of High-Severity ClamAV Vulnerabilities With Public PoC	https://securityweek.com/cisco-warns-of-high-severity-clamav-vulnerabilities-with-public-poc
TrueConf Server Flaws Exploited to Replace Client Installers with PhantomCore	https://thehackernews.com/2026/08/head-mare-exploits-trueconf-flaws-to.html
Critical Progress LoadMaster flaw now actively exploited in attacks	https://bleepingcomputer.com/news/security/cisa-warns-of-critical-progress-loadmaster-flaw-exploited-in-attacks

CISA Urges Immediate Patching of Exploited Progress LoadMaster Vulnerability	https://securityweek.com/cisa-urges-immediate-patching-of-exploited-progress-loadmaster-vulnerability
Critical Flaws Discovered in Belgian eID Software Used by 2 Million People	https://securityweek.com/critical-flaws-discovered-in-belgian-eid-software-used-by-2-million-people
Metabase 0-Day Vulnerability Exploited in the Wild to Gain Admin Access	https://cybersecuritynews.com/metabase-0-day-vulnerability
Critical One-Click Vulnerability in Atlassian's Rovo AI Exposed Enterprise Data	https://securityweek.com/critical-one-click-vulnerability-in-atlassians-rovo-ai-exposed-enterprise-data
Metabase Zero-Day Exploited in Wild Allows Admin Access Without Authentication	https://thehackernews.com/2026/08/metabase-zero-day-exploited-in-wild.html
Progress Kemp LoadMaster Flaw Hits CISA KEV After 792 Reported Exploit Attempts	https://thehackernews.com/2026/08/progress-kemp-loadmaster-flaw-hits-cisa.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
Metabase Patches Vulnerability Exploited as Zero-Day	https://securityweek.com/metabase-patches-vulnerability-exploited-as-zero-day
N-able Issues N-central Hotfix 2 as Attackers Reach Managed Systems and Persist	https://thehackernews.com/2026/08/n-central-attackers-reach-managed.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
New Phishing Attack Leverage SSL/TLS Certificates to Target High-value Brands Customers Via Whatsapp	https://cybersecuritynews.com/new-phishing-attack
BdThemes Supply Chain Attack Poisons JSON to Create Rogue WordPress Admins	https://thehackernews.com/2026/08/bdthemes-supply-chain-attack-poisons.html
New StormEncryptor ransomware used by former Medusa affiliate	https://bleepingcomputer.com/news/security/new-stormencryptor-ransomware-used-by-former-medusa-affiliate
Gunra Ransomware Exploits Fortinet VPN Flaws to Bypass MFA and Steal Enterprise Data	https://cybersecuritynews.com/gunra-ransomware-exploits-fortinet-vpn-flaws
China-Linked Hackers Deploy New StormEncryptor Ransomware, Likely via N-central Flaw	https://thehackernews.com/2026/08/china-linked-hackers-deploy-new.html
GitHub Expands Supply Chain Malware Detection From npm to 8 Package Registries	https://cybersecuritynews.com/github-expands-supply-chain-malware-detection
CISA: SonicWall SMA1000 flaws now exploited by ransomware gangs	https://bleepingcomputer.com/news/security/cisa-sonicwall-sma1000-flaws-now-exploited-by-ransomware-gangs

Σύντομη περιγραφή / Τίτλος	URL
Ransomware Operators Disable EDR, Backup Software and Windows Telemetry Before Encryption	https://cybersecuritynews.com/ransomware-operators-disable-edr
New Passkey Attacks Can Recover Synced Private Keys or Bypass Phishing-Resistant MFA	https://thehackernews.com/2026/08/new-passkey-attacks-can-recover-synced.html
Kimsuky Uses Local LLMs, AI-Generated Lures and GitHub C2 to Deploy AsyncRAT	https://cybersecuritynews.com/kimsuky-uses-local-llms
Go-Based macOS Malware Steals Crypto and Secrets	https://infosecurity-magazine.com/news/gobased-macos-malware-crypto-and
Payroll Pirates AiTM Phishing Hijacks Microsoft 365 Sessions and Targets Payroll Emails	https://cybersecuritynews.com/payroll-pirates-aitm-phishing
New Wordpress Supply Chain Attack Compromises Themes via Poisoned API Response	https://cybersecuritynews.com/wordpress-supply-chain-attack

Guides / Tools

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

Σύντομη περιγραφή / Τίτλος	URL
Top 10 Malware Threats of the Week – AsyncRAT, Remcos, and Xworm Lead the Surge	https://cybersecuritynews.com/top-10-malware-threats

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 08/08/2026–11/08/2026 και έχει γίνει μια επιλογή συστημάτων/υπηρεσιών ανάλογα με το πόσο διαδεδομένα είναι.

Annex – Websites with vendor specific vulnerabilities

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

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