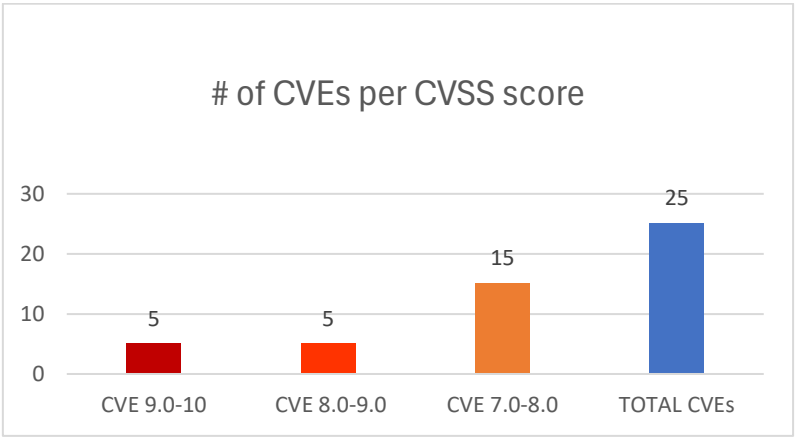
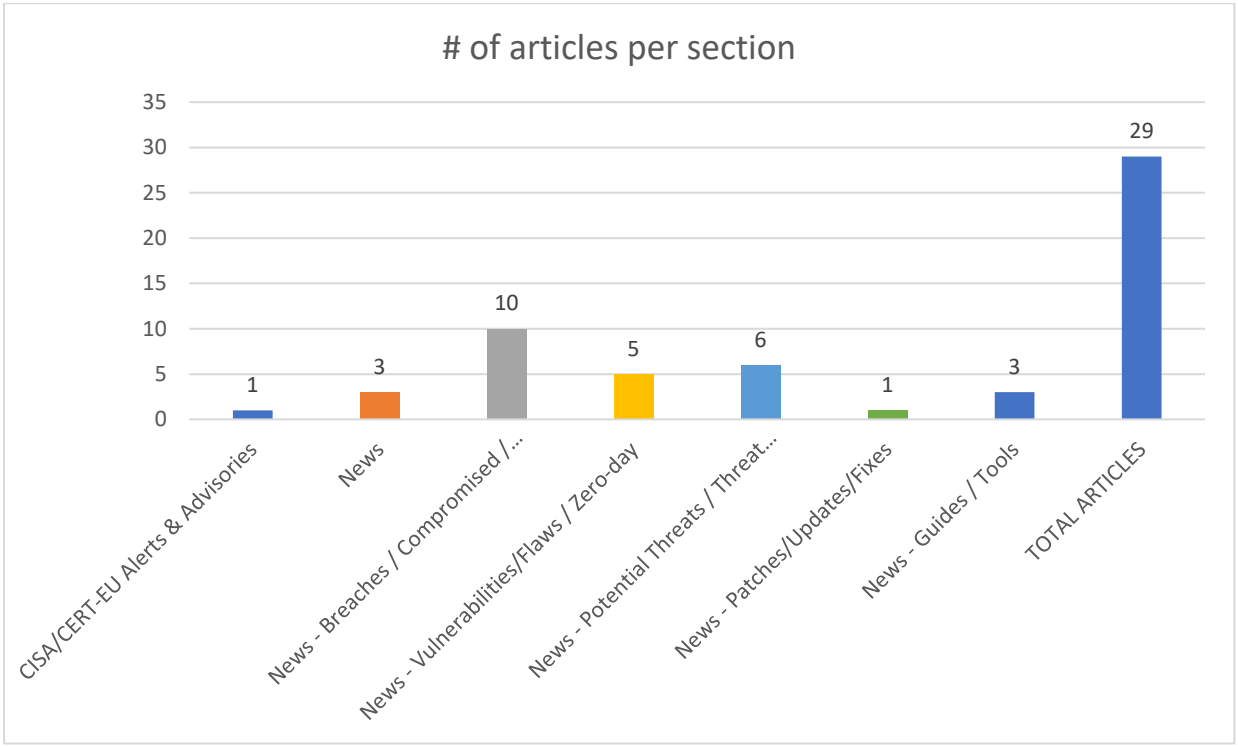
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 15/08/2025 - 19/08/2025





Contents

Common Vulnerabilities and Exposures (CVEs)

URL ευπάθειας (NIST NVD)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2025-7441	9,8	The StoryChief plugin for WordPress	Unrestricted Upload of File with Dangerous Type	in all versions up to, and including, 1.0.42	https://plugins.trac.wordpress.org/browser/story-chief/trunk/includes/tools.php#L75 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/979efaa4-10f1-4c7f-b4b0-5a41678c9d66?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-6679	9,8	The Bit Form builder plugin for WordPress	Unrestricted Upload of File with Dangerous Type	in all versions up to, and including, 2.20.4	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3343461%40bit-form%2Ftrunk&old=3336733%40bit-form%2Ftrunk&sfp_email=&sfph_mail= Wordfence https://wordpress.org/plugins/bit-form/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/6e2e294f-904b-4674-8baf-d3a9a260d634?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-7778	9,8	The Icons Factory plugin for WordPress	Improper Authorization	in all versions up to, and including, 1.6.12	https://plugins.trac.wordpress.org/browser/icons-factory/tags/1.6.12/icons-factory.php#L1330 Wordfence https://wordpress.org/plugins/icons-factory/#developers Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/24f31bbf-883f-4903-847a-7bfc3e45654c?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-8995	9,8	Drupal Authenticator Login allows Authentication Bypass.	Authentication Bypass Using an Alternate Path or Channel	from 0.0.0 before 2.1.4	https://www.drupal.org/sa-contrib-2025-096
https://nvd.nist.gov/vuln/detail/CVE-2025-9060	9,1	MSoft MFlash application	Improper Input Validation	v. 8.0	https://github.com/klsecservices/Advisories/blob/master/K-MSoft-2025-002.md
https://nvd.nist.gov/vuln/detail/CVE-2025-49895	8,8	iThemes ServerBuddy by PluginBuddy.Com	Cross-Site Request Forgery (CSRF)	from n/a through 1.0.5	https://patchstack.com/database/wordpress/plugin/serverbuddy-by-pluginbuddy/vulnerability/wordpress-serverbuddy-by-pluginbuddy-com-plugin-1-0-5-csrf-to-php-object-injection-vulnerability?_s_id=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-3671	8,8	The WPGYM - Wordpress Gym Management System plugin for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	in all versions up to, and including, 67.7.0	https://codecanyon.net/item/-wpgym-wordpress-gym-management-system/13352964 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/6536d19f-a042-4404-b0c9-91aacd7768f7?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-9006	8,8	Tenda CH22	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	1.0.0.1	https://github.com/moweizhang1994/cve/issues/2 CISA-ADP, VulDB Exploit Issue Tracking Third Party Advisory https://vuldb.com/?ctiid.320035 VulDB Permissions Required https://vuldb.com/?id.320035 VulDB Third Party Advisory VDB Entry https://vuldb.com/?submit.628845 VulDB Third Party Advisory VDB Entry https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-9023	8,8	Tenda AC7 and AC18	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	15.03.05.19/15.03.06.44	https://github.com/zezhifu1/cve_report/blob/main/AC18/formsetschedled.md VulDB https://github.com/zezhifu1/cve_report/blob/main/AC7/formsetschedled.md VulDB https://vuldb.com/?ctiid.320088 VulDB https://vuldb.com/?id.320088 VulDB https://vuldb.com/?submit.629692 VulDB https://vuldb.com/?submit.629696 VulDB https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2025-8342	8,1	The WooCommerce OTP Login With Phone Number	Missing Authorization	in all versions up to, and including, 1.8.47	https://plugins.trac.wordpress.org/browser/login-with-phone-number/tags/1.8.47/login-with-phonenumber.php#L4358 Wordfence https://plugins.trac.wordpress.org/browser/login-with-phone-number/tags/1.8.47/login-with-phonenumber.php#L4373 Wordfence https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3338150%40login-with-phone-number&new=3338150%40login-with-phone-number&sfp_email=&sfph_mail= Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/6e74582f-8e94-4cba-a3eb-0a823a5235ad?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-5046	7,8	Autodesk AutoCAD	Out-of-bounds Read		https://www.autodesk.com/products/autodesk-access/overview Autodesk https://www.autodesk.com/trust/security-advisories/adsk-sa-2025-0017
https://nvd.nist.gov/vuln/detail/CVE-2025-8092	7,6	Drupal COOKiES Consent Management	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	from 0.0.0 before 1.2.16	https://www.drupal.org/sa-contrib-2025-092
https://nvd.nist.gov/vuln/detail/CVE-2025-8959	7,5	HashiCorp's go-getter library	Improper Link Resolution Before File Access ('Link Following')		https://discuss.hashicorp.com/t/hcsec-2025-23-hashicorp-go-getter-vulnerable-to-arbitrary-read-through-symlink-attack/76242
https://nvd.nist.gov/vuln/detail/CVE-2024-12612	7,5	The School Management System for Wordpress plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	in all versions up to, and including, 93.2.0	https://codecanyon.net/item/school-management-system-for-wordpress/11470032 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/258877a7-670c-4a3c-8107-47dc7ba6a5ed?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-7641	7,5	The Assistant for NextGEN Gallery plugin for WordPress	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	in all versions up to, and including, 1.0.9	http://plugins.trac.wordpress.org/browser/assistant-for-nextgen-gallery/trunk/nextgenassistant.php#L163 Wordfence https://wordpress.org/plugins/assistant-for-nextgen-gallery/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/07ebb176-a1f8-4a5c-8d81-a83fda4b0af3?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-9087	7,4	Tenda AC20	Stack-based Buffer Overflow	16.03.08.12	https://github.com/ZZ2266/.github.io/tree/main/AC20/formSetQosBand VulDB https://github.com/ZZ2266/.github.io/tree/main/AC20/formSetQosBand#poc-python-exploit-script VulDB https://vuldb.com/?ctiid.320355 VulDB https://vuldb.com/?id.320355 VulDB https://vuldb.com/?submit.632037 VulDB https://www.tenda.com.cn/

https://nvd.nist.gov/vuln/detail/CVE-2025-8983	7,3	Online Tour and Travel Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/zhuyi-hz/cve/issues/8 CISA-ADP, VulDB Exploit Issue Tracking Third Party Advisory https://itsourcecode.com/ VulDB Product https://vuldb.com/?ctiid.319979 VulDB Permissions Required VDB Entry https://vuldb.com/?id.319979 VulDB Third Party Advisory VDB Entry https://vuldb.com/?submit.628660
https://nvd.nist.gov/vuln/detail/CVE-2025-8986	7,3	SourceCodester COVID 19 Testing Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/zhuyi-hz/cve/issues/5 CISA-ADP, VulDB Exploit Issue Tracking Third Party Advisory https://vuldb.com/?ctiid.319982 VulDB Permissions Required VDB Entry https://vuldb.com/?id.319982 VulDB Third Party Advisory VDB Entry https://vuldb.com/?submit.628663 VulDB Third Party Advisory VDB Entry https://www.sourcecodester.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-9002	7,3	Surbowl dormitory-management-php		Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	https://github.com/fatdog957/CVE-/issues/1 CISA-ADP, VulDB https://vuldb.com/?ctiid.320031 VulDB https://vuldb.com/?id.320031 VulDB https://vuldb.com/?submit.625595
https://nvd.nist.gov/vuln/detail/CVE-2025-9012	7,3	PHPGurukul Online Shopping Portal Project	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	2.0	https://github.com/StrongDog23/myCVE/issues/2 VulDB https://phpgurukul.com/ VulDB https://vuldb.com/?ctiid.320043 VulDB https://vuldb.com/?id.320043 VulDB https://vuldb.com/?submit.629456
https://nvd.nist.gov/vuln/detail/CVE-2025-9021	7,3	SourceCodester Online Bank Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to 1.0	https://vuldb.com/?ctiid.320086 VulDB https://vuldb.com/?id.320086 VulDB https://vuldb.com/?submit.631861 VulDB https://www.sourcecodester.com/

https://nvd.nist.gov/vuln/detail/CVE-2025-9024	7,3	PHPGurukul Beauty Parlour Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.1	https://github.com/StrongDog23/myCVE/issues/4 VulDB https://phpgurukul.com/ VulDB https://vuldb.com/?ctiid.320089 VulDB https://vuldb.com/?id.320089 VulDB https://vuldb.com/?submit.629773
https://nvd.nist.gov/vuln/detail/CVE-2025-9027	7,3	Online Medicine Guide	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ VulDB https://github.com/Jackie1732/CVE/issues/2 VulDB https://vuldb.com/?ctiid.320092 VulDB https://vuldb.com/?id.320092 VulDB https://vuldb.com/?submit.630187
https://nvd.nist.gov/vuln/detail/CVE-2025-24975	7,1	Firebird	Improper Check for Unusual or Exceptional Conditions	Prior to snapshot versions 4.0.6.3183, 5.0.2.1610, and 6.0.0.609	https://github.com/FirebirdSQL/firebird/commit/658abd20449f72097fbbce57e8e6ae42ff837fb6 GitHub, Inc. https://github.com/FirebirdSQL/firebird/issues/8429 GitHub, Inc. https://github.com/FirebirdSQL/firebird/security/advisories/GHSA-fx9r-rj68-7p69
https://nvd.nist.gov/vuln/detail/CVE-2025-9016	7,0	Mechrevo Control Center	Untrusted Search Path	GX V2 5.56.51.48	https://drive.proton.me/urls/7QYSEW6734#H3N4fQ3mw6gX VulDB https://vuldb.com/?ctiid.320067 VulDB https://vuldb.com/?id.320067 VulDB https://vuldb.com/?submit.624900

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2025-54948 Trend Micro Apex One OS Command Injection Vulnerability	https://www.cisa.gov/news-events/alerts/2025/08/18/cisa-adds-one-known-exploited-vulnerability-catalog

News

Σύντομη περιγραφή / Τίτλος	URL
Russian Group EncryptHub Exploits MSC EvilTwin Vulnerability to Deploy Fickle Stealer Malware	https://thehackernews.com/2025/08/russian-group-encrypthub-exploits-msc.html
CFE Data Leak Exposes 600GB Of Internal Logs of Mexico's Power Operations	https://dailysecurityreview.com/security-spotlight/cfe-data-leak-exposes-600gb-of-internal-logs-of-mexicos-power-operations/
Man Jailed for 20 Months After Compromising Millions of Accounts	https://www.infosecurity-magazine.com/news/man-jailed-20-months-millions-of/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
DoJ Seizes $2.8 Million in Crypto From Zeppelin Ransomware Operators	https://cybersecuritynews.com/doj-seizes-2-8-million-in-crypto/
Threats Actors Using Telegram as The Communication Channel to Exfiltrate The Stolen Data	https://cybersecuritynews.com/threats-actors-using-telegram-as-the-communication-channel/
ERMAC v3.0 Banking Malware Source Code Exposed via Weak Password 'changemeplease'	https://cybersecuritynews.com/ermac-v3-0-banking-malware-source-code-exposed/
HR giant Workday discloses data breach after Salesforce attack	https://www.bleepingcomputer.com/news/security/hr-giant-workday-discloses-data-breach-amid-salesforce-attacks/
Critical PostgreSQL Vulnerabilities Allow Arbitrary Code Injection During Restoration	https://cybersecuritynews.com/critical-postgresql-vulnerabilities/
Popular npm Package Compromised in Phishing Attack	https://www.infosecurity-magazine.com/news/popular-npm-package-compromised-in/
Human resources firm Workday disclosed a data breach	https://securityaffairs.com/181271/data-breach/human-resources-firm-workday-disclosed-a-data-breach.html?&web_view=true
WestJet Data Breach Exposes Passenger Details, Including Names, DOB and Travel Details	https://dailysecurityreview.com/security-spotlight/westjet-data-breach-exposes-passenger-details-including-names-dob-and-travel-details/
HR Giant Workday Discloses Data Breach After Hackers Compromise Third-Party CRM	https://cybersecuritynews.com/workday-data-breach/
Hundreds of TeslaMate Installations Leaking Sensitive Vehicle Data in Real Time	https://cybersecuritynews.com/teslamate-leaks-vehicle-data/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Microsoft Windows Vulnerability Exploited to Deploy PipeMagic RansomExx Malware	https://thehackernews.com/2025/08/microsoft-windows-vulnerability.html
Fortinet FortiSIEM Command Injection Vulnerability (CVE-2025-25256) – Technical Details Revealed	https://cybersecuritynews.com/fortinet-fortisiem-command-injection-vulnerability/
Multiple ImageMagick Vulnerabilities Cause Memory Corruption and Integer Overflows	https://cybersecuritynews.com/multiple-imagemagick-vulnerabilities/
New Elastic EDR 0-Day Vulnerability Allows Attackers to Bypass Detection, Execute Malware, and Cause BSOD	https://cybersecuritynews.com/elastic-edr-0-day-vulnerability/
Linux Kernel Netfilter Vulnerability Let Attackers Escalate Privileges	https://cybersecuritynews.com/linux-kernel-netfilter-vulnerability/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Cisco Patches Critical Vulnerability in Firewall Management Platform	https://www.securityweek.com/cisco-patches-critical-vulnerability-in-firewall-management-platform/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Weaponized Python Package Termncolor Attacking Leverages Windows Run Key to Maintain Persistence	https://cybersecuritynews.com/weaponized-python-package-termncolor/
Hackers Exploit Cisco Secure Links to Evade Link Scanners and Bypass Network Filters	https://cybersecuritynews.com/hackers-weaponizing-ciscos-secure-links/
Over 800 N-able servers left unpatched against critical flaws	https://www.bleepingcomputer.com/news/security/over-800-n-able-servers-left-unpatched-against-critical-flaws/
Taiwan Web Infrastructure targeted by APT UAT-7237 with custom toolset	https://securityaffairs.com/181195/apt/taiwan-web-infrastructure-targeted-by-apt-uat-7237-with-custom-toolset.html
Colt Customers Face Prolonged Outages After Major Cyber Incident	https://www.infosecurity-magazine.com/news/colt-outages-after-major-cyber/?&web_view=true
Threat Actor Allegedly Claiming Access to 15.8 Million PayPal Email and Passwords in Plaintext	https://cybersecuritynews.com/paypal-email-and-passwords-leak/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Top Tools for Enterprise Security Monitoring	**https://cybersecuritynews.com/enterprise-security-monitoring-tools/**
10 Best Vulnerability Management Tools In 2025	https://cybersecuritynews.com/vulnerability-management-tools/
10 Best API Protection Tools in 2025	https://cybersecuritynews.com/best-api-protection-tools/

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 CVSSv3 score >= 7.0 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/