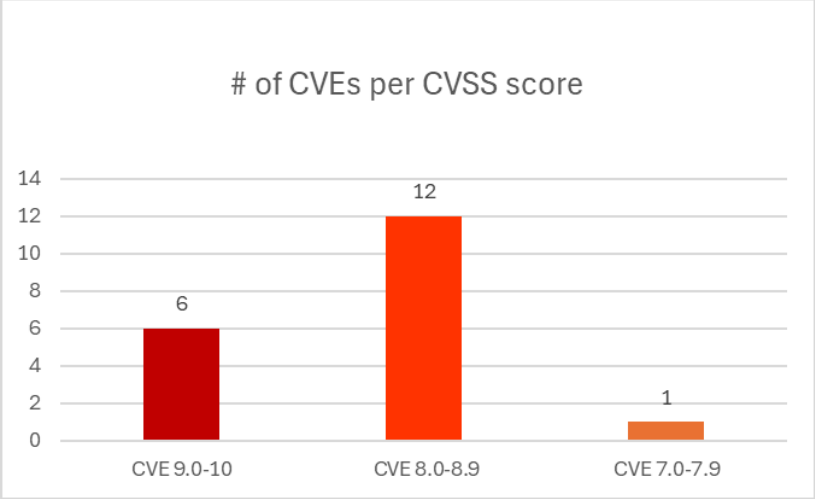
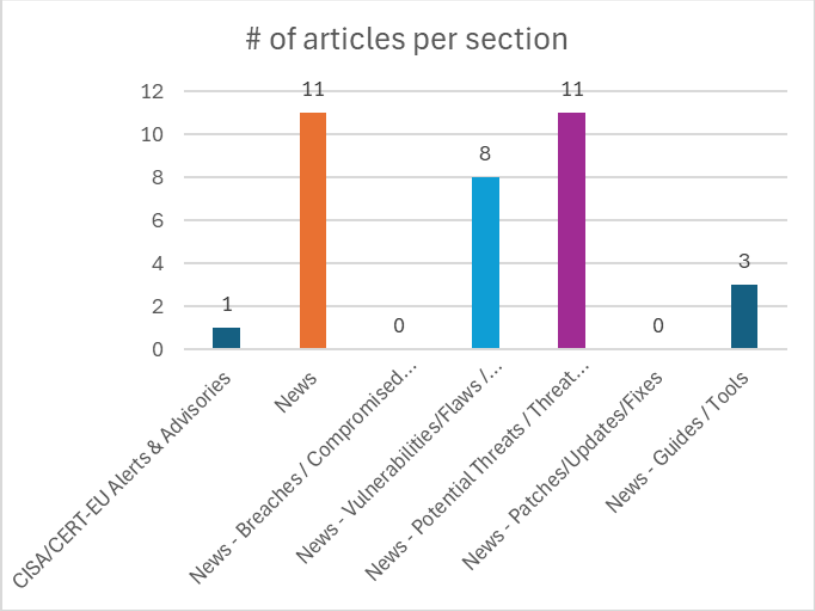
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 28/03/2026 - 31/03/2026





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 της ευπάθειας (όπως SQL injection ή command injection) και σχετικοί σύνδεσμοι για περαιτέρω πληροφόρηση ή μέτρα αντιμετώπισης.

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-2026-32987	9,8	OpenClaw	Authentication Bypass by Capture-replay	OpenClaw before 2026.3.13	https://github.com/openclaw/openclaw/commit/1803d16d5cec970c54b0e1ac46b31b1cbade335c https://github.com/openclaw/openclaw/security/advisories/GHSA-63f5-hhc7-cx6p https://www.vulncheck.com/advisories/openclaw-bootstrap-setup-code-replay-via-device-pairing
https://nvd.nist.gov/vuln/detail/CVE-2026-33032	9,8	Nginx	Missing Authentication for Critical Function	Nginx UI is a web user interface for the Nginx web server. In versions 2.3.5 and prior	https://github.com/0xJacky/nginx-ui/security/advisories/GHSA-h6c2-x2m2-mwhf
https://nvd.nist.gov/vuln/detail/CVE-2026-4176	9,8	Perl		Perl versions from 5.9.4 before 5.40.4-RC1, from 5.41.0 before 5.42.2-RC1, from 5.43.0 before 5.43.9	http://www.openwall.com/lists/oss-security/2026/03/30/2 https://github.com/Perl/perl5/commit/c75ae9cc164205e1b6d6dbd57bd2c65c8593fe94 https://lists.security.metacpan.org/cve-announce/msg/37638919/ https://metacpan.org/release/PMQS/Compress-Raw-Zlib-2.221/source/Changes https://metacpan.org/release/SHAY/perl-5.40.4/changes https://metacpan.org/release/SHAY/perl-5.42.2/changes https://www.cve.org/CVERecord?id=CVE-2026-3381
https://nvd.nist.gov/vuln/detail/CVE-2026-5020	9,8	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink A3600R 4.1.2cu.5182_B20201102	https://lavender-bicycle-a5a.notion.site/TOTOLINK_A3600R_setNoticeCfg-32253a41781f80c197eaf8e7558c5ed1?source=copy_link https://vuldb.com/submit/779536 https://vuldb.com/vuln/353905 VulDB https://vuldb.com/vuln/353905/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-5030	9,8	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink NR1800X 9.1.0u.6279_B20210910	https://lavender-bicycle-a5a.notion.site/TOTOLINK-NR1800X-NTPSyncWithHost-32153a41781f8032afebc0802b704e9c?source=copy_link https://vuldb.com/submit/778529 https://vuldb.com/vuln/353952 VulDB https://vuldb.com/vuln/353952/cti https://www.totolink.net/
https://www.cve.org/CVERecord?id=CVE-2026-3055	9,3	NetScaler	Out-of-bounds Read	NetScaler ADC and NetScaler Gateway	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696300

https://nvd.nist.gov/vuln/detail/CVE-2026-5036	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda 4G06 04.06.01.29	https://github.com/Kiciot/cve/issues/1 https://vuldb.com/submit/778625 https://vuldb.com/vuln/353962 VulDB https://vuldb.com/vuln/353962/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-5044	8,8	Belkin	Out-of-bounds Write	Belkin F9K1122 1.00.33	https://github.com/Litengzheng/vul_db/blob/main/Belkin/vul_155/README.md VulDB https://vuldb.com/submit/779125 https://vuldb.com/vuln/353967 VulDB https://vuldb.com/vuln/353967/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-5046	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda FH1201 1.2.0.14(408)	https://github.com/Litengzheng/vul_db/blob/main/FH1201/vul_44/README.md VulDB https://vuldb.com/submit/779127 https://vuldb.com/vuln/353969 VulDB https://vuldb.com/vuln/353969/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-5101	8,8	Totolink	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Totolink A3300R 17.0.0cu.557_b20221024	https://github.com/Litengzheng/vul_db/blob/main/A3300R/vul_39/README.md VulDB https://vuldb.com/submit/779128 https://vuldb.com/vuln/354126 VulDB https://vuldb.com/vuln/354126/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-5102	8,8	Totolink	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	Totolink A3300R 17.0.0cu.557_b20221024	https://github.com/Litengzheng/vul_db/blob/main/A3300R/vul_40/README.md VulDB https://vuldb.com/submit/779129 https://vuldb.com/vuln/354127 VulDB https://vuldb.com/vuln/354127/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-5103	8,8	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink A3300R 17.0.0cu.557_b20221024	https://github.com/LvHongW/Vuln-of-totolink_A3300R/tree/main/A3300R_enable_cmd_inject https://vuldb.com/submit/779140 https://vuldb.com/vuln/354128 VulDB https://vuldb.com/vuln/354128/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-5104	8,8	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink A3300R 17.0.0cu.557_b20221024	https://github.com/LvHongW/Vuln-of-totolink_A3300R/tree/main/A3300R_ip_cmd_inject https://vuldb.com/submit/779142 https://vuldb.com/vuln/354129 VulDB https://vuldb.com/vuln/354129/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-5105	8,8	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink A3300R 17.0.0cu.557_b20221024	https://github.com/LvHongW/Vuln-of-totolink_A3300R/tree/main/A3300R_pptpPassThru_cmd_inject https://vuldb.com/submit/779143 https://vuldb.com/vuln/354130 VulDB

					https://vuldb.com/vuln/354130/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-5152	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda CH22 1.0.0.1	https://github.com/Litengzheng/vuldb_new/blob/main/CH22/vul_50/README.md https://vuldb.com/submit/780203 https://vuldb.com/vuln/354184 https://vuldb.com/vuln/354184/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-5154	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda CH22 1.0.0.1	https://github.com/Litengzheng/vuldb_new/blob/main/CH22/vul_48/README.md https://vuldb.com/submit/780206 https://vuldb.com/vuln/354186 https://vuldb.com/vuln/354186/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-5155	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda CH22 1.0.0.1	https://github.com/Litengzheng/vuldb_new/blob/main/CH22/vul_47/README.md https://vuldb.com/submit/780207 https://vuldb.com/vuln/354187 https://vuldb.com/vuln/354187/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-5156	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda CH22 1.0.0.1	https://github.com/Litengzheng/vuldb_new/blob/main/CH22/vul_46/README.md https://vuldb.com/submit/780208 https://vuldb.com/vuln/354188 https://vuldb.com/vuln/354188/cti https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-5176	7,3	Totolink	Improper Neutralization of Special Elements in Output Used by a Down-stream Component ('Injection')	Totolink A3300R 17.0.0cu.557_b20221024	https://github.com/LvHongW/Vuln-of-totolink_A3300R/tree/main/A3300R_rtLogServer_cmd_inject https://vuldb.com/submit/779145 https://vuldb.com/vuln/354244 https://vuldb.com/vuln/354244/cti https://www.totolink.net/

CISA/CERT-EU Alerts & Advisories

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

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2026-3055 Citrix NetScaler Out-of-Bounds Read Vulnerability	https://www.cisa.gov/news-events/alerts/2026/03/30/cisa-adds-one-known-exploited-vulnerability-catalog

News

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

Σύντομη περιγραφή / Τίτλος	URL
Notepad++ v8.9.3 Released Addressing cURL Security Vulnerability and Crash Issues	https://cybersecuritynews.com/notepad-v8-9-3-released/
Axios NPM Packages Compromised to Inject Malicious Codes in an Active Supply Chain Attack	https://cybersecuritynews.com/axios-npm-packages-compromised/
TeamPCP Supply Chain Attack Allegedly Compromised Databricks Platform	https://cybersecuritynews.com/databricks-teampcp-supply-chain/
India Set to Ban Sale of Hikvision, TP-Link, CCTV Products From April	https://cybersecuritynews.com/india-ban-cctv-products/
New “Prompt Poaching” Attack Steals Users’ AI Conversations via Malicious Browser Extensions	https://cybersecuritynews.com/prompt-poaching-attack/
Microsoft Issues Critical WinRE and Setup Updates Ahead of 2026 Secure Boot Certificate Expiration	https://cybersecuritynews.com/microsoft-critical-winre-update/
Hackers Probe Citrix NetScaler Instances Ahead of Likely CVE-2026-3055 Exploitation	https://cybersecuritynews.com/citrix-netscaler-instances-exploited/
Cybersecurity Companies’ Stocks Fall as Anthropic Tests Powerful New Model	https://cybersecuritynews.com/cybersecurity-stocks-anthropic/
European Commission Confirms Cyberattack Following AWS Account Hack	https://cybersecuritynews.com/european-commission-aws-hack/
Windows 11 and Server 2025 Update to Block Untrusted Cross-Signed Kernel Drivers by Default	https://cybersecuritynews.com/windows-11-and-server-2025-update/
FBI Chief Kash Patel’s Gmail Account was Hacked by Iranian Hackers	https://cybersecuritynews.com/fbi-chief-kash-patel-gmail-hacked/

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

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
Claude AI Discovers Zero-Day RCE Vulnerabilities in Vim and Emacs	https://cybersecuritynews.com/claude-ai-0-day-rce-vim/
Stored XSS Bug in Jira Work Management Could Lead to Full Organization Takeover	https://cybersecuritynews.com/stored-xss-bug-in-jira-work-management/
Vim Vulnerability Let Attackers Execute Arbitrary Command Via Weaponized Files	https://cybersecuritynews.com/vim-vulnerability/
Critical Grafana Vulnerabilities Let Attackers Achieve Remote Code Execution	https://cybersecuritynews.com/grafana-vulnerabilities-rce/
Critical n8n Vulnerability Let Attackers Achieve Remote Code Execution	https://cybersecuritynews.com/n8n-vulnerability/
Critical Fortinet Forticlient EMS Vulnerability Exploited in Attacks	https://cybersecuritynews.com/forticlient-ems-vulnerability-exploited/
CISA Warns of F5 BIG-IP Vulnerability Actively Exploited in Attacks	https://cybersecuritynews.com/f5-big-ip-vulnerability-actively-exploited/
CISA Adds Aquasecurity Trivy Scanner Vulnerability to KEV Catalog	https://cybersecuritynews.com/aquasecurity-trivy-scanner-vulnerability/

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

Potential threats / Threat intelligence

Η συγκεκριμένη ενότητα ασχολείται με νέες απειλές, εξελιγμένα malware και τεχνικές επιθέσεων που έχουν εντοπιστεί σε πραγματικές συν-θήκες. Περι-λαμβάνονται αναφορές σε εργαλεία που χρησιμοποιούν οι επιτιθέμενοι, αλλά και δείκτες (IoCs) που μπορούν να χρησιμοποιηθούν στην άμυνα.

Σύντομη περιγραφή / Τίτλος	URL
Exposed Server Reveals TheGentlemen Ransomware Toolkit, Victim Credentials, and Ngrok Tokens	https://cybersecuritynews.com/exposed-server-reveals-thegentlemen-ransomware-toolkit/
North Korean IT Worker Allegedly Used Stolen Identity and AI Resume in Job Appli-cation Scam	https://cybersecuritynews.com/north-korean-it-worker-allegedly-used-stolen-identity/
CrySome RAT Emerges as Advanced .NET Malware With AV Killer and HVNC Capabil-ities	https://cybersecuritynews.com/crysome-rat-emerges-as-advanced-net-malware/
New ClickFix Variant Uses Rundll32 and WebDAV to Evade PowerShell Detection	https://cybersecuritynews.com/new-clickfix-variant-uses-rundll32/
TA446 Hackers Deploying DarkSword Exploit Kit to Attack iOS Users	https://cybersecuritynews.com/ta446-hackers-deploying-darksword-exploit-kit/
New Homoglyph Attack Techniques Help Cybercriminals Spoof Trusted Domains	https://cybersecuritynews.com/new-homoglyph-attack-techniques/
Hackers Backdoor Telnyx Python SDK on PyPI to Steal Cloud and Dev Credentials	https://cybersecuritynews.com/hackers-backdoor-telnyx-python-sdk/
Open VSX's New Scanner Vulnerability Allows Malicious Extension Goes Live	https://cybersecuritynews.com/open-vsxs-new-scanner-vulnerability/
BlankGrabber Stealer Uses Fake Certificate Loader to Hide Malware Delivery Chain	https://cybersecuritynews.com/blankgrabber-stealer-uses-fake-certificate-loader/
CanisterWorm Malware Attacking Docker/K8s/Redis to Gain Access and Steal Se-crets	https://cybersecuritynews.com/canisterworm-malware-attacking-docker/
VoidLink Malware Framework Shows that AI-assisted Malware is Not Experimental Anymore	https://cybersecuritynews.com/voidlink-malware-framework-2/

Guides / Tools

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

Σύντομη περιγραφή / Τίτλος	URL
10 Best Spam Filter Tools 2026	https://cybersecuritynews.com/best-spam-filter-tools/
10 Best Log Monitoring Tools in 2026	https://cybersecuritynews.com/best-log-monitoring-tools/
10 Best Fraud Detection Tools in 2026	https://cybersecuritynews.com/best-fraud-detection-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/