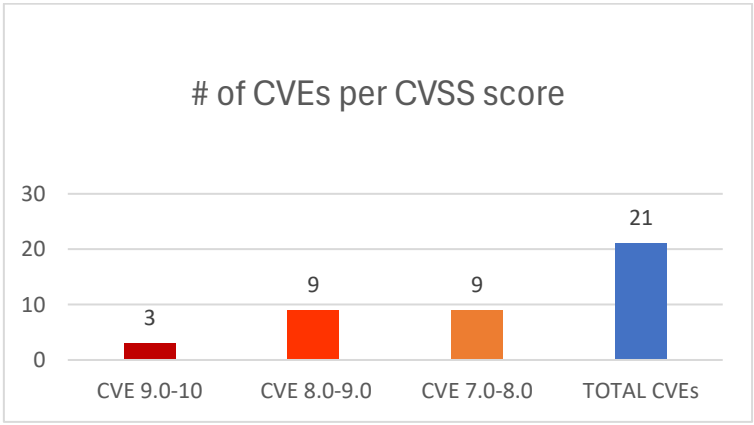
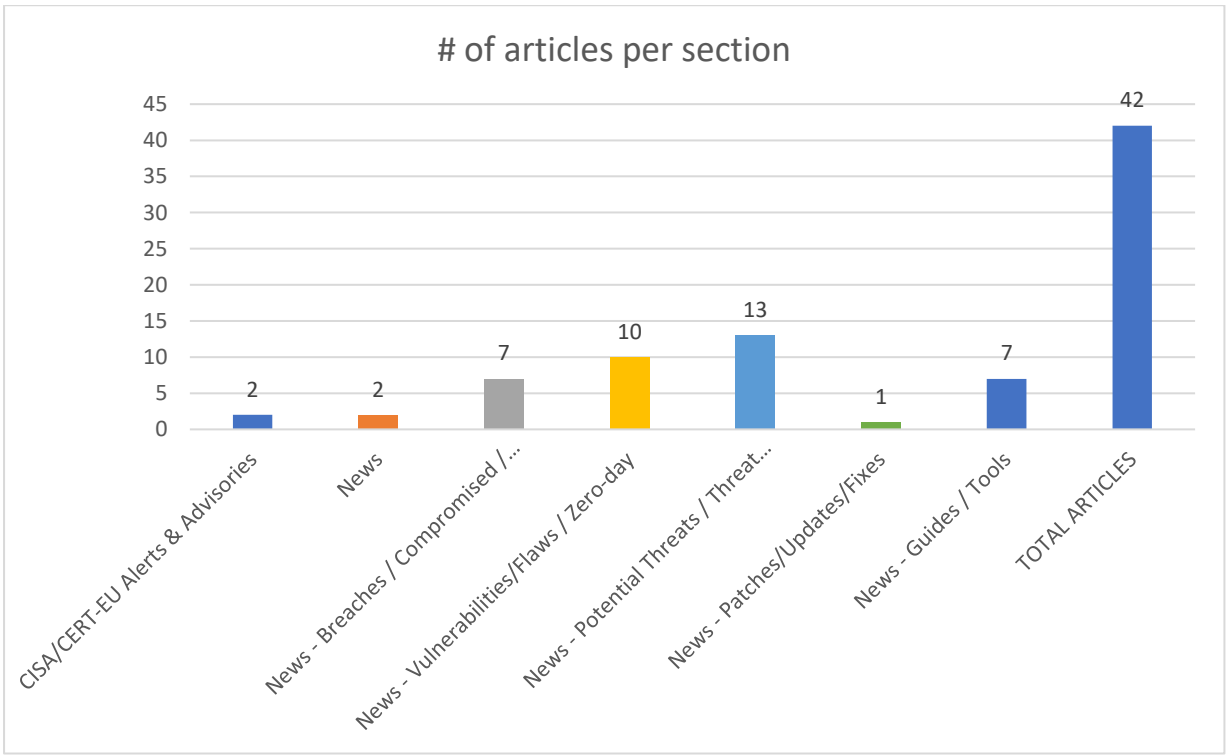
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 14/11/2025 - 18/11/2025





Contents

Common Vulnerabilities and Exposures (CVEs) 3
CISA/CERT-EU Alerts & Advisories 7
News 8
Breaches / Compromised / Hacked 8
Vulnerabilities / Flaws / Zero-day 9
Patches / Updates / Fixes 9
Potential threats / Threat intelligence 10
Guides / Tools 11
References 12
Annex – Websites with vendor specific vulnerabilities 13

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-2025-64446	9,8	Fortinet	Relative Path Traversal	FortiWeb 8.0.0 through 8.0.1, FortiWeb 7.6.0 through 7.6.4, FortiWeb 7.4.0 through 7.4.9, FortiWeb 7.2.0 through 7.2.11, FortiWeb 7.0.0 through 7.0.11	https://fortiguard.fortinet.com/psirt/FG-IR-25-910 Fortinet, Inc. Vendor Advisory https://github.com/watchtowrlabs/watchTowr-vs-Fortiweb-AuthBypass CISA-ADP Exploit Third Party Advisory https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2025-64446
https://nvd.nist.gov/vuln/detail/CVE-2025-40547	9,1	Serv-U	Improper Encoding or Escaping of Output		https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_15-5-3_release_notes.htm SolarWinds https://www.solarwinds.com/trust-center/security-advisories/CVE-2025-40547
https://nvd.nist.gov/vuln/detail/CVE-2025-9501	9,0	The W3 Total Cache WordPress plugin	command injection	before 2.8.13	https://wpscan.com/vulnerability/6697a2c9-63ae-42f0-8931-f2e5d67d45ae/
https://nvd.nist.gov/vuln/detail/CVE-2025-8693	8,8	Zyxel DX3300-T0 firmware	Improper Neutralization of Special Elements used in an OS Command ('OS	5.50(ABVY.6.3)C0 and earlier	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-uncontrolled-resource-consumption-and-command-injection-vulnerabilities-in-certain-4g-lte-5g-nr-cpe-dsl-ethernet-cpe-fiber-onts-

			Command Injection')		security-routers-and-wireless-extenders-11-18-2025
https://nvd.nist.gov/vuln/detail/CVE-2025-63748	8,8	QaTraq	Unrestricted Upload of File with Dangerous Type	6.9.2	http://qatraq.com MITRE https://bitsby-amg.com/blog/post/2025/10/19/qatraq-692-default-creds-and-file-upload-rce
https://nvd.nist.gov/vuln/detail/CVE-2025-36553	8,8	CvManager functionality of Dell ControlVault3	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	Dell ControlVault3 prior to 5.15.14.19 and Dell ControlVault3 Plus prior to 6.2.36.47	https://talosintelligence.com/vulnerability_reports/TALOS-2025-2189 Talos https://www.dell.com/support/kbdoc/en-us/000326061/dsa-2025-228 Talos https://www.talosintelligence.com/vulnerability_reports/TALOS-2025-2189
https://nvd.nist.gov/vuln/detail/CVE-2025-13319	8,8	Digi On-Prem Manager	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')		https://dom.nettec.no/security-advisories/DOM-25-001/
https://nvd.nist.gov/vuln/detail/CVE-2025-13305	8,8	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	DWR-M920, DWR-M921, DWR-M960, DIR-822K and DIR-825M 1.01.07	https://github.com/LX-LX88/cve/issues/12 VulDB https://vuldb.com/?ctiid.332645 VulDB https://vuldb.com/?id.332645 VulDB https://vuldb.com/?submit.691809 VulDB https://vuldb.com/?submit.691816 VulDB https://vuldb.com/?submit.693784 VulDB https://vuldb.com/?submit.693806 VulDB https://vuldb.com/?submit.695424 VulDB https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-31361	8,7	ControlVault WBDI Driver	Use of Uninitialized Resource	Dell ControlVault3 prior to 5.15.14.19 and Dell ControlVault3 Plus prior to 6.2.36.47	https://talosintelligence.com/vulnerability_reports/TALOS-2025-2174 Talos https://www.dell.com/support/kbdoc/en-us/000326061/dsa-2025-228 Talos

		WBIO_USH_ADD_REC-ORD			https://www.talosintelligence.com/vulnerability_reports/TALOS-2025-2174
https://nvd.nist.gov/vuln/detail/CVE-2025-64309	8,6	Brightpick Mission Control	Unprotected Transport of Credentials		https://brightpick.ai/contact-us/ ICS-CERT https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2025/icsa-25-317-04.json ICS-CERT https://www.cisa.gov/news-events/ics-advisories/icsa-25-317-04
https://nvd.nist.gov/vuln/detail/CVE-2025-9317	8,4	Edge Project files or Edge Offline Cache files	Use of a Broken or Risky Cryptographic Algorithm		https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2025/icsa-25-317-03.json ICS-CERT https://www.aveva.com/content/dam/aveva/documents/support/cyber-security-updates/SecurityBulletin_AVEVA-2025-006.pdf ICS-CERT https://www.cisa.gov/news-events/ics-advisories/icsa-25-317-03
https://nvd.nist.gov/vuln/detail/CVE-2025-36357	8,0	IBM Planning Analytics Local	Absolute Path Traversal	2.1.0 through 2.1.14	https://www.ibm.com/support/pages/node/7251265
https://nvd.nist.gov/vuln/detail/CVE-2025-40936	7,8	PS/IGES Parasolid Translator Component	Out-of-bounds Read	All versions < V29.0.258	https://cert-portal.siemens.com/productcert/html/ssa-241605.html
https://nvd.nist.gov/vuln/detail/CVE-2025-65073	7,5	OpenStack Keystone	Incorrect Authorization	before 26.0.1, 27.0.0, and 28.0.0	http://www.openwall.com/lists/oss-security/2025/11/17/6 CVE https://www.openwall.com/lists/oss-security/2025/11/04/2

https://nvd.nist.gov/vuln/detail/CVE-2025-64756	7,5	the glob CLI	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10.3.7 to 11.0.3	https://github.com/isaacs/node-glob/commit/47473c046b91c67269df7a66eab782a6c2716146 GitHub, Inc. https://github.com/isaacs/node-glob/security/advisories/GHSA-5j98-mcp5-4vw2
https://nvd.nist.gov/vuln/detail/CVE-2025-62765	7,5	General Industrial Controls Lynx+ Gateway	Cleartext Transmission of Sensitive Information		https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2025/icsa-25-317-08.json ICS-CERT https://www.cisa.gov/news-events/ics-advisories/icsa-25-317-08
https://nvd.nist.gov/vuln/detail/CVE-2025-36118	7,5	IBM Storage Virtualize	Improper Clearing of Heap Memory Before Release ('Heap Inspection')	8.4, 8.5, 8.7, and 9.1 IKEv1	https://www.ibm.com/support/pages/node/7250954
https://nvd.nist.gov/vuln/detail/CVE-2025-58407	7,4	Kernel	Time-of-check Time-of-use (TOCTOU) Race Condition	-	https://www.imaginationtech.com/gpu-driver-vulnerabilities/
https://nvd.nist.gov/vuln/detail/CVE-2025-13323	7,3	Simple Pizza Ordering System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ VulDB https://github.com/daojian1/Simple-Pizza-Ordering-System_V1.0_003 VulDB https://vuldb.com/?ctiid.332662 VulDB https://vuldb.com/?id.332662 VulDB https://vuldb.com/?submit.691844

https://nvd.nist.gov/vuln/detail/CVE-2025-62519	7,2	phpMyFAQ is an open source FAQ web application	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Prior to version 4.0.14	https://github.com/thorsten/phpMyFAQ/compare/4.0.13...4.0.14 GitHub, Inc. https://github.com/thorsten/phpMyFAQ/security/advisories/GHSA-fxm2-cmwj-qvx4
https://nvd.nist.gov/vuln/detail/CVE-2025-63917	7,1	PDFPatcher	Improper Restriction of XML External Entity Reference	1.1.3.4663	https://github.com/cydtseng/Vulnerability-Research/blob/main/pdfpatcher/XXE-Importers.md MITRE https://github.com/wmjordan/PDFPatcher MITRE https://www.cnblogs.com/pdfpatcher

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
Fortinet Releases Security Advisory for Relative Path Traversal Vulnerability Affecting FortiWeb Products	CVE-2025-64446 ▪ 8.0.0 through 8.0.1 ▪ 7.6.0 through 7.6.4 ▪ 7.4.0 through 7.4.9 ▪ 7.2.0 through 7.2.11 ▪ 7.0.0 through 7.0.11	https://www.cisa.gov/news-events/alerts/2025/11/14/fortinet-releases-security-advisory-relative-path-traversal-vulnerability-affecting-fortiweb
CISA Adds One Known Exploited Vulnerability to Catalog	CVE-2025-64446	https://www.cisa.gov/news-events/alerts/2025/11/14/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
Unremovable Spyware on Samsung Devices Comes Pre-installed on Galaxy Series Devices	https://cybersecuritynews.com/spyware-on-samsung-devices/
Hackers Allegedly Claim Leak of LG Source Code, SMTP, and Hardcoded Credentials	https://cybersecuritynews.com/lg-data-leak-claim/

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
Chinese Tech Firm Leak Reportedly Exposes State Linked Hacking	https://hackread.com/chinese-tech-firm-leak-state-linked-hacking/?&web_view=true
Washington Post data breach impacts nearly 10K employees, contractors	https://www.bleepingcomputer.com/news/security/washington-post-data-breach-impacts-nearly-10k-employees-contractors/?&web_view=true
Record-Breaking 15 Tbps DDoS Attack From 500,000+ Devices Hits Azure Network	https://cybersecuritynews.com/ddos-attack-azure-network
North Korean Hackers Infiltrated 136 U.S. Companies to Generate $2.2 Million in Revenue	https://cybersecuritynews.com/north-korean-hackers-infiltrated-u-s-companies/
Akira Ransomware Targets Over 250 Organizations, Extracts $42 Million in Ransom Payments – New CISA Report	https://cybersecuritynews.com/akira-ransomware-targets-over-250-organizations/
Malicious npm Package with 206k Downloads Attacking GitHub-Owned Repositories to Exfiltrate Tokens	https://cybersecuritynews.com/malicious-npm-package-with-206k-downloads/
CISA Warns of Critical Lynx+ Gateway Vulnerability Exposes Data in Cleartext	https://cybersecuritynews.com/lynx-gateway-vulnerability/

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
RondoDox Exploits Unpatched XWiki Servers to Pull More Devices Into Its Botnet	https://thehackernews.com/2025/11/rondodox-exploits-unpatched-xwiki.html
Now-Patched Fortinet FortiWeb Flaw Exploited in Attacks to Create Admin Accounts	https://thehackernews.com/2025/11/fortinet-fortiweb-flaw-actively.html
Imunify360 Vulnerability Could Expose Millions of Sites to Hacking	https://www.securityweek.com/imunify360-vulnerability-could-expose-millions-of-sites-to-hacking/
DoorDash email spoofing vulnerability sparks messy disclosure dispute	https://www.bleepingcomputer.com/news/security/doordash-email-spoofing-vulnerability-sparks-messy-disclosure-dispute/
IBM AIX Vulnerabilities Let Remote Attacker Execute Arbitrary Commands	https://cybersecuritynews.com/ibm-aix-vulnerabilities/
Chrome Type Confusion Zero-Day Vulnerability Actively Exploited in the Wild	https://cybersecuritynews.com/chrome-type-confusion-zero-day/
New MobileGestalt Exploit for iOS 26.0.1 Enables Unauthorized Writes to Protected Data	https://cybersecuritynews.com/mobilegestalt-exploit-ios-26-0-1/
Cisco Catalyst Center Vulnerability Let Attackers Escalate Priveleges	https://cybersecuritynews.com/cisco-catalyst-center-vulnerability/
Critical pgAdmin4 Vulnerability Lets Attackers Execute Remote Code on Servers	https://cybersecuritynews.com/pgadmin4-vulnerability/
NVIDIA NeMo Framework Vulnerabilities Allows Code Injection and Privilege Escalation	https://cybersecuritynews.com/nvidia-nemo-framework-vulnerabilities/

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
Google Issues Security Fix for Actively Exploited Chrome V8 Zero-Day Vulnerability	https://thehackernews.com/2025/11/google-issues-security-fix-for-actively.html

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
Kraken Uses Benchmarking to Enhance Ransomware Attacks	https://www.infosecurity-magazine.com/news/kraken-benchmarking-enhance/
Chinese Hackers Automate Cyber-Attacks With AI-Powered Claude Code	https://www.infosecurity-magazine.com/news/chinese-hackers-cyberattacks-ai/
Threat Actors Leveraging Compromised RDP Logins to Deploy Lynx Ransomware After Deleting Server Backups	https://cybersecuritynews.com/threat-actors-leveraging-compromised-rdp-logins-to-deploy-lynx/
Threat Actors can Use Xanthorox AI Tool to Generate Different Malicious Code Based on Prompts	https://cybersecuritynews.com/threat-actors-can-use-xanthorox-ai-tool/
Payroll Pirates – Network of Criminal Groups Hijacking Payroll Systems	https://cybersecuritynews.com/payroll-pirates-network-of-criminal-groups/
Yurei Ransomware File Encryption, Operation Model and Data Transfer Methods Uncovered	https://cybersecuritynews.com/yurei-ransomware-file-encryption/
Pig-Butchering Scams Operators Scaled Their Operations with The Support of AI-Assistants	https://cybersecuritynews.com/pig-butchering-scams-operators/
EVALUSION Campaign Using ClickFix Technique to deploy Amatera Stealer and NetSupport RAT	https://cybersecuritynews.com/evalusion-campaign-using-clickfix-technique/
Critical RCE Vulnerabilities in AI Inference Engines Exposes Meta, Nvidia and Microsoft Frameworks	https://cybersecuritynews.com/ai-inference-engines-rce-vulnerabilities/
Iranian SpearSpecter Attacking High-Value Officials Using Personalized Social Engineering Tactics	https://cybersecuritynews.com/iranian-spearspecter-attacking-high-value-officials/
Hackers are Weaponizing Invoices to Deliver XWorm That Steals Login Credentials	https://cybersecuritynews.com/hackers-are-weaponizing-invoices-to-deliver-xworm/
Highly Sophisticated macOS DigitStealer Employs Multi-Stage Attacks to Evade detection	https://cybersecuritynews.com/highly-sophisticated-macos-digitstealer/
Lumma Stealer Uses Browser Fingerprinting to Collect Data and for Stealthy C&C Server Communications	https://cybersecuritynews.com/lumma-stealer-uses-browser-fingerprinting/

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 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/
Splunk Releases Guide to Detect Remote Employment Fraud Within Your Organization	https://cybersecuritynews.com/detect-remote-employment-fraud/
Top 15 Best Security Incident Response Tools In 2025	https://cybersecuritynews.com/incident-response-tools/
10 Best API Protection Tools in 2025	https://cybersecuritynews.com/best-api-protection-tools/
ThreatBook Launches Best-of-Breed Advanced Threat Intelligence Solution	https://cybersecuritynews.com/threatbook-advanced-threat-intelligence-solution/
CISA Releases Best Security Practices Guide for Hardening Microsoft Exchange Server	https://cybersecuritynews.com/microsoft-exchange-server-hardening-guide/

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/