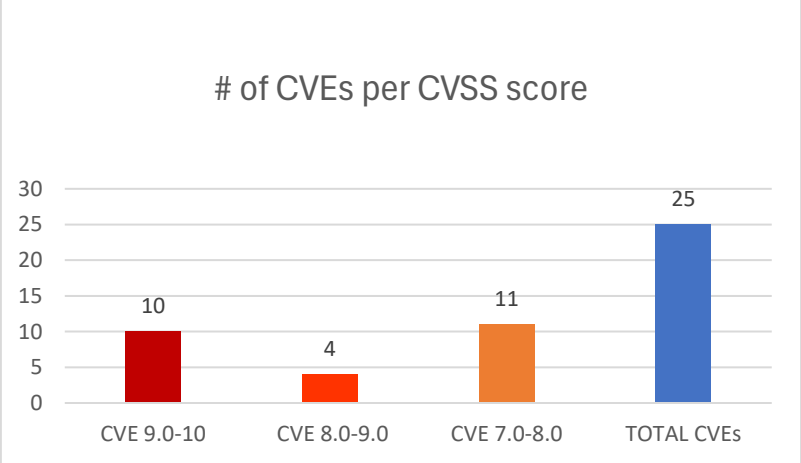
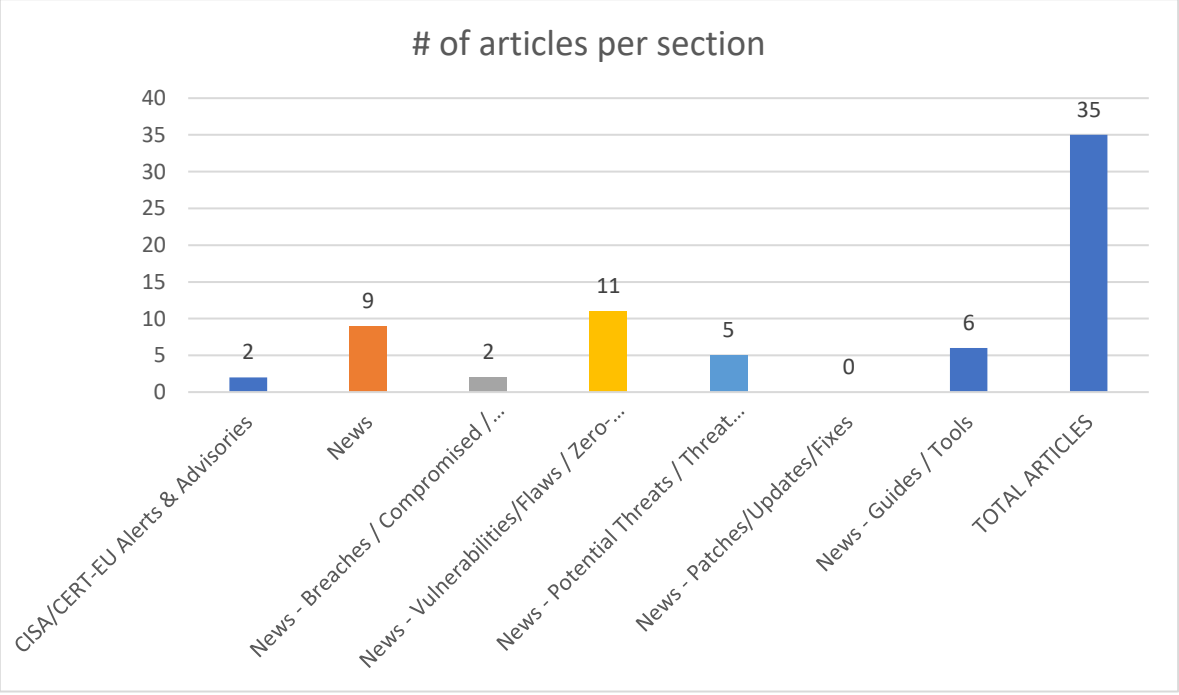
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 17/12/2025 - 19/12/2025





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-2025-65041	10,0	Microsoft Partner Center	Improper Authorization		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-65041
https://nvd.nist.gov/vuln/detail/CVE-2025-65037	10,0	Azure Container Apps	Improper Control of Generation of Code ('Code Injection')		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-65037
https://nvd.nist.gov/vuln/detail/CVE-2025-67781	9,9	DriveLock	Improper Privilege Management	24.1 before 24.1.6, 24.2 before 24.2.7, and 25.1 before 25.1.5	https://drivelock.help/en-us/Content/Home.htm
https://nvd.nist.gov/vuln/detail/CVE-2025-67164	9,9	Pagekit CMS	Improper Control of Generation of Code ('Code Injection')	v1.0.18	https://github.com/mbiesiad/vulnerability-research/tree/main/CVE-2025-67164
https://nvd.nist.gov/vuln/detail/CVE-2025-67895	9,8	Apache Airflow Providers Edge3	Incorrect Resource Transfer Between Spheres	before 2.0.0	http://www.openwall.com/lists/oss-security/2025/12/16/3 CVE https://github.com/apache/airflow/pull/59143 Apache Software Foundation https://lists.apache.org/thread/hhnmmzkj5qx5gbk6pdkh8tcsx5oj1nqs

https://nvd.nist.gov/vuln/detail/CVE-2025-67073	9,8	Tenda	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	AC10V4.0 V16.03.10.20	https://github.com/johnathanhuutri/CVEReport/tree/master/CVE-2025-67073
https://nvd.nist.gov/vuln/detail/CVE-2025-65008	9,4	WODESYS WD-R608U router	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	-	http://www.wodesys.com/eproductms52.html CERT.PL https://cert.pl/en/posts/2025/12/CVE-2025-65007 CERT.PL https://github.com/wcyb/security_research
https://nvd.nist.gov/vuln/detail/CVE-2025-68400	9,3	ChurchCRM	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	prior to version 6.5.3	https://github.com/ChurchCRM/CRM/security/advisories/GHSA-v54g-2pvg-gvp2
https://nvd.nist.gov/vuln/detail/CVE-2025-68435	9,1	Zerobyte	Authentication Bypass by Primary Weakness	prior to 0.18.5 and 0.19.0	https://github.com/nicotsx/zerobyte/commit/13e080a18967705bd2b4e110e5f7693fdca1c692 GitHub, Inc. https://github.com/nicotsx/zerobyte/issues/161 GitHub, Inc. https://github.com/nicotsx/zerobyte/security/advisories/GHSA-x539-c98q-38gv
https://nvd.nist.gov/vuln/detail/CVE-2025-68398	9,1	Weblate	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	prior to 5.15.1	https://github.com/WeblateOrg/weblate/pull/17330 GitHub, Inc. https://github.com/WeblateOrg/weblate/pull/17345 GitHub, Inc. https://github.com/WeblateOrg/weblate/releases/tag/weblate-5.15.1 GitHub, Inc. https://github.com/WeblateOrg/weblate/security/advisories/GHSA-8vcg-cfxj-p5m3
https://nvd.nist.gov/vuln/detail/CVE-2025-68434	8,8	Open Source Point of Sale (opensourcepos)	Cross-Site Request Forgery (CSRF)	3.4.0 and prior to version 3.4.2	https://github.com/Nixon-H/CVE-2025-68434-OSPOS-CSRF-Unauthorized-Administrator-Creation CISA-ADP, GitHub, Inc. Exploit Third Party Advisory

					https://github.com/opensourcepos/open-sourcepos/com-mit/d575c8da9a1d7af8313a1e758e000e243f5614ef GitHub, Inc. Patch https://github.com/opensourcepos/open-sourcepos/pull/4349 GitHub, Inc. Issue Tracking https://github.com/opensourcepos/open-sourcepos/security/advisories/GHSA-wjm4-hfwg-5w
https://nvd.nist.gov/vuln/de-tail/CVE-2025-66953	8,8	Uplink Power Contril Unit	Cross-Site Request Forgery (CSRF)	UPC2 v.1.17	https://github.com/shiky8/my--cve-vulnera-bility-research/tree/main/CVE-2025-66953%20_%20narda%20miteq%20Up-link%20Power%20Con-tril%20Unitl%20UPC2%20_%20CSRF CISA-ADP, MITRE https://www.nardamiteq.com/
https://nvd.nist.gov/vuln/de-tail/CVE-2025-67843	8,3	MDX Rendering Engine in Mintlify Platform	Improper Neutralization of Special Elements Used in a Template En-gine	before 2025-11-15	https://kibty.town/blog/mintlify/ MITRE https://news.ycombina-tor.com/item?id=46317098 MITRE https://www.mintlify.com/blog/working-with-security-researchers-november-2025 MITRE https://www.mintlify.com/docs/changelog
https://nvd.nist.gov/vuln/de-tail/CVE-2025-68147	8,1	Open Source Point of Sale	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	3.4.0 and prior to version 3.4.2	https://github.com/Nixon-H/CVE-2025-68147-OSPOS-Stored-XSS CISA-ADP, GitHub, Inc. Exploit Third Party Advisory https://github.com/opensourcepos/open-sourcepos/commit/22297a GitHub, Inc. Patch https://github.com/opensourcepos/open-sourcepos/security/advisories/GHSA-xgr7-7pvw-fpmh

https://nvd.nist.gov/vuln/detail/CVE-2025-68433	7,7	Zed	Improper Neutralization of Special Elements used in a Command ('Command Injection')	prior to 0.218.2-pre	https://github.com/zed-industries/zed/security/advisories/GHSA-cv6g-cmxc-vw8j GitHub, Inc. https://zed.dev/blog/secure-by-default
https://nvd.nist.gov/vuln/detail/CVE-2025-7358	7,5	SoliClub	Use of Hard-coded Credentials	before 5.3.7	https://www.usom.gov.tr/bildirim/tr-25-0466
https://nvd.nist.gov/vuln/detail/CVE-2025-67493	7,5	Homarr	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	Prior to version 1.45.3	https://github.com/homarr-labs/homarr/security/advisories/GHSA-59gp-q3xx-489q
https://nvd.nist.gov/vuln/detail/CVE-2025-67171	7,5	RiteCMS	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	v3.1.0	https://github.com/handylulu/RiteCMS/ MITRE Product https://github.com/mbiesiad/vulnerability-research/tree/main/CVE-2025-67171
https://nvd.nist.gov/vuln/detail/CVE-2025-66070	7,5	wpForo Forum	Missing Authorization	from n/a through <= 2.4.10	https://vdp.patchstack.com/database/Wordpress/Plugin/wpforo/vulnerability/wordpress-wpforo-forum-plugin-2-4-10-broken-access-control-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-68429	7,3	Storybook	Insertion of Sensitive Information into Externally-Accessible File or Directory	7.0.0 and prior to versions 7.6.21, 8.6.15, 9.1.17, and 10.1.10	https://github.com/storybookjs/storybook/security/advisories/GHSA-8452-54wp-rmv6 GitHub, Inc. https://storybook.js.org/blog/security-advisory
https://nvd.nist.gov/vuln/detail/CVE-2025-68461	7,2	Roundcube Webmail	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	before 1.5.12 and 1.6 before 1.6.12	https://github.com/roundcube/roundcubemail/commit/bfa032631c36b900e7444dfa278340b33cbf7cdb MITRE https://roundcube.net/news/2025/12/13/security-updates-1.6.12-and-1.5.12

https://nvd.nist.gov/vuln/detail/CVE-2025-68459	**7,2**	RG - AP180, Indoor Wall Plate Wireless AP AP180 series	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')		https://jvn.jp/en/vu/JVNVU94068946/ JPCERT/CC https://www.ruijie.com.cn/gy/xw-aqtg-gw/930282/
https://nvd.nist.gov/vuln/detail/CVE-2025-68385	**7,2**		Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')		https://discuss.elastic.co/t/kibana-8-19-9-9-1-9-and-9-2-3-security-update-esa-2025-34/384182
https://nvd.nist.gov/vuln/detail/CVE-2025-67745	**7,1**	MyHoard	Transmission of Private Resources into a New Sphere ('Resource Leak')	1.0.1 and prior to version 1.3.0	https://github.com/Aiven-Open/myhoard/commit/fac89793bfc8c81ae040aadf5292f5d0100b6640 GitHub, Inc. https://github.com/Aiven-Open/myhoard/security/advisories/GHSA-v42r-6hr9-4hcr
https://nvd.nist.gov/vuln/detail/CVE-2025-65203	**7,1**	KeePassXC-Browser	Cross-Site Request Forgery (CSRF)		https://github.com/keepassxreboot/keepassxc-browser/issues/2647 MITRE https://github.com/keepassxreboot/keepassxc-browser/pull/2648

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 Releases Nine Industrial Control Systems Advisories	▪ **ICSA-25-352-01 Inductive Automation Ignition** ▪ **ICSA-25-352-02 Schneider Electric EcoStruxure Foxboro DCS Advisor** ▪ **ICSA-25-352-03 National Instruments LabView** ▪ **ICSA-25-352-04 Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electrics Products** ▪ **ICSA-25-352-05 Siemens Interniche IP-Stack** ▪ **ICSA-25-352-06 Advantech WebAccess/SCADA** ▪ **ICSA-25-352-07 Rockwell Automation Micro820, Micro850, Micro 870** ▪ **ICSA-25-352-08 Axis Communications Camera Station Pro, Camera Station, and Device Manager** ▪ **ICSA-24-291-03 Mitsubishi Electric CNC Series (Update C)**	**https://www.cisa.gov/news-events/alerts/2025/12/18/cisa-releases-nine-industrial-control-systems-advisories**
CISA Adds Three Known Exploited Vulnerabilities to Catalog	▪ **CVE-2025-20393 Cisco Multiple Products Improper Input Validation Vulnerability** ▪ **CVE-2025-40602 SonicWall SMA1000 Missing Authorization Vulnerability** ▪ **CVE-2025-59374 ASUS Live Update Embedded Malicious Code Vulnerability**	**https://www.cisa.gov/news-events/alerts/2025/12/17/cisa-adds-three-known-exploited-vulnerabilities-catalog**

News

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

Σύντομη περιγραφή / Τίτλος	URL
Dormant Iran APT is Still Alive, Spying on Dissidents	https://www.darkreading.com/threat-intelligence/iran-apt-spying-dissidents
In Cybersecurity, Claude Leaves Other LLMs in the Dust	https://www.darkreading.com/cybersecurity-analytics/cybersecurity-claude-llms
China-Aligned APT Hackers Exploit Windows Group Policy to Deploy Malware	https://cybersecuritynews.com/china-aligned-apt-hackers-exploit-windows-group-policy/
OpenAI GPT-5.2-Codex Supercharges Agentic Coding and Vulnerability Detection	https://cybersecuritynews.com/gpt-5-2-codex/
Amazon Catches North Korean IT Worker by Tracking Tiny 110ms Keystroke Delays	https://cybersecuritynews.com/amazon-catches-north-korean-it-worker/
Researchers Uncovered New Lazarus and Kimsuky Infrastructure with Active Tools and Tunnel-ling Nodes	https://cybersecuritynews.com/researchers-uncovered-new-lazarus-and-kimsuky/
Chinese-based Ink Dragon Compromises Asia and South America into European Government Networks	https://cybersecuritynews.com/chinese-based-ink-dragon-compromises-asia/
North Korea Steals Over $2bn in Crypto in 2025	https://www.infosecurity-magazine.com/news/north-korea-steals-over-2bn-crypto/
European Investigators Disrupt $12m Call Center Fraud Ring	https://www.infosecurity-magazine.com/news/european-investigators-12m-call/

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
Richmond, VA mental health service notifies 113,000+ people of data breach	https://www.comparitech.com/news/richmond-va-mental-health-service-notifies-113000-people-of-data-breach/?&web_view=true
Kimwolf Android Botnet Hijacked 1.8 Million Android Devices Worldwide	https://cybersecuritynews.com/kimwolf-android-botnet-hijacked/

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
HPE OneView Flaw Rated CVSS 10.0 Allows Unauthenticated Remote Code Execution	https://thehackernews.com/2025/12/hpe-oneview-flaw-rated-cvss-100-allows.html
CISA Flags Critical ASUS Live Update Flaw After Evidence of Active Exploitation	https://thehackernews.com/2025/12/cisa-flags-critical-asus-live-update.html
Cisco Warns of Active Attacks Exploiting Unpatched 0-Day in AsyncOS Email Security Appliances	https://thehackernews.com/2025/12/cisco-warns-of-active-attacks.html
SonicWall Fixes Actively Exploited CVE-2025-40602 in SMA 100 Appliances	https://thehackernews.com/2025/12/sonicwall-fixes-actively-exploited-cve.html
Critical React2Shell flaw exploited in ransomware attacks	https://www.bleepingcomputer.com/news/security/critical-react2shell-flaw-exploited-in-ransomware-attacks/
Critical Fortinet Flaws Under Active Attack	https://www.darkreading.com/cyberattacks-data-breaches/critical-fortinet-flaws-under-active-attack
Critical Apache Commons Text Vulnerability Enables Remote Code Execution Attacks	https://cybersecuritynews.com/apache-commons-text-vulnerability/
Critical Vulnerability in Popular Node.js Library Exposes Windows Systems to RCE Attacks	https://cybersecuritynews.com/node-js-library-exposes-windows/
Motors WordPress Vulnerability Exposes Sites to Takeover	https://www.infosecurity-magazine.com/news/motors-wordpress-flaw-takeover/
CISA Warns of Gladinet CentreStack and Triofox Vulnerability Exploited in Attacks	https://cybersecuritynews.com/gladinet-centrestack-and-triofox-vulnerability/
NVIDIA Isaac Lab Vulnerability Let Attackers Execute Malicious Code	https://cybersecuritynews.com/nvidia-isaac-lab-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 συνθήκες. Περιλαμβάνονται αναφορές σε εργαλεία που χρησιμοποιούν οι επιτιθέμενοι, αλλά και δείκτες (IoCs) που μπορούν να χρησιμοποιηθούν στην άμυνα.

Σύντομη περιγραφή / Τίτλος	URL
New Udados Botnet Launches Massive HTTP Flood DDoS Attacks Targeting Tech Sector	**https://cybersecuritynews.com/udados-botnet-ddos-attack/**
Hackers Hijacking VNC Connections to Gain Access to OT Control Devices in Critical Infrastructure	**https://cybersecuritynews.com/hackers-hijacking-vnc-connections/**
Microsoft 365 Services Including Teams, Outlook and Copilot Outage Hits Users in Japan and China	**https://cybersecuritynews.com/microsoft-365-services-and-copilot-outage/**
Kimsuky Hackers Attacking Users via Weaponized QR Code to Deliver Malicious Mobile App	**https://cybersecuritynews.com/kimsuky-hackers-attacking-users/**
Urban VPN Proxy Accused of Harvesting AI Chat Conversations	**https://www.infosecurity-magazine.com/news/urban-vpn-proxy-harvesting-ai-chats/**

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/

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/