NATIONAL CYBERSECURITY AUTHORITY GR

CVEs Alerts

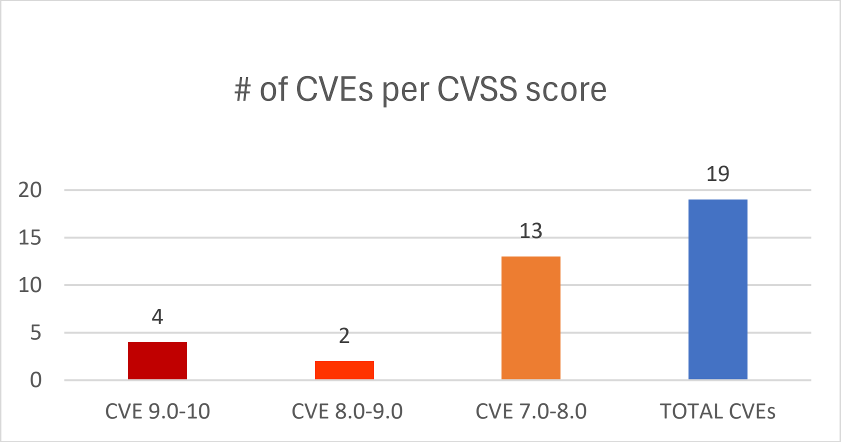
CVEs, CISA/CERT-EU Alerts Advisories & News

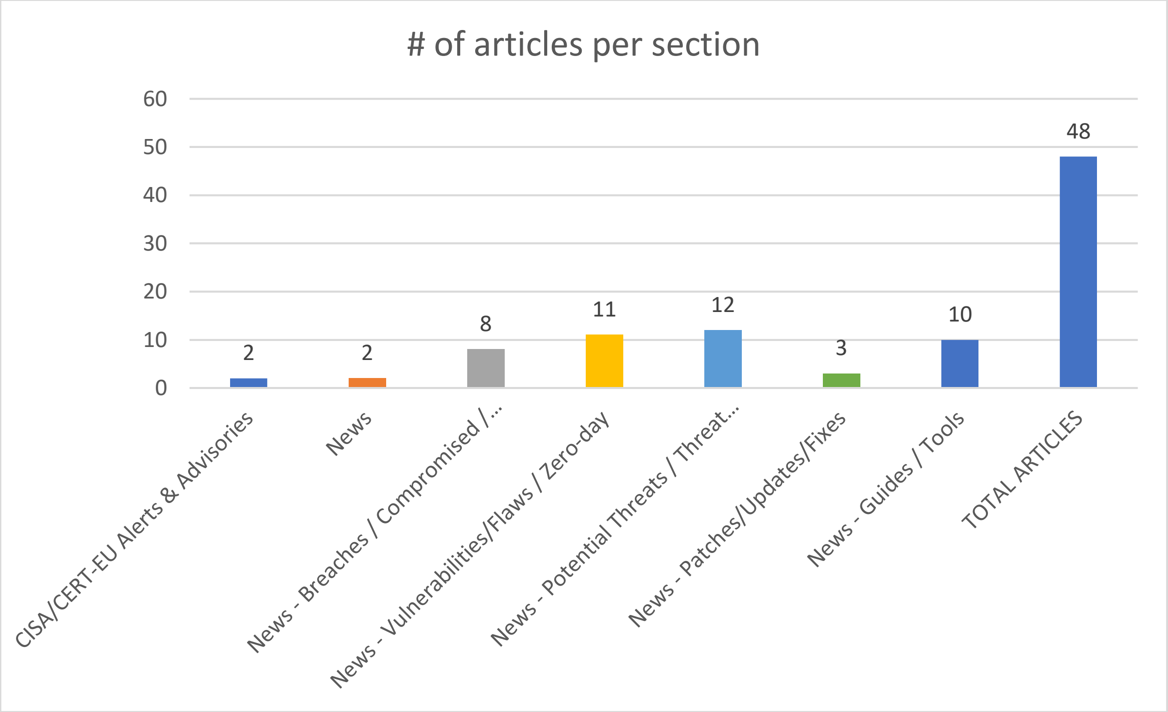
Newsletter on system vulnerabilities and cybersecurity news

Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

**Date: 28/01/2026 - 30/01/2026**





# 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) | CVSSv 3 | Προϊόν/Υπηρεσία | Τύπος Ευπάθειας | Συσκευές/Εκδόσεις που επηρεάζονται | URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης |
|---|---|---|---|---|---|
| https://nvd.nist.gov/vuln/detail/CVE-2026-24897 | 10,0 | Erugo | Improper Control of Generation of Code ('Code Injection') | up to and including 0.2.14 | https://github.com/ErugoOSS/Erugo/commit/256bc63831a0b5e9a94cb024a0724e0cd5fa5e38 GitHub, Inc.<br>https://github.com/ErugoOSS/Erugo/releases/tag/v0.2.15 GitHub, Inc.<br>https://github.com/ErugoOSS/Erugo/security/advisories/GHSA-336w-hgpq-6369 |
| https://nvd.nist.gov/vuln/detail/CVE-2026-1699 | 10,0 | Eclipse Theia Website repository | Inclusion of Functionality from Untrusted Control Sphere | - | https://gitlab.eclipse.org/security/vulnerability-reports/-/issues/332 |
| https://nvd.nist.gov/vuln/detail/CVE-2026-1453 | 9,8 | KiloView Encoder Series | Missing Authentication for Critical Function | | https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-029-01.json ICS-CERT<br>https://www.cisa.gov/news-events/ics-advisories/icsa-26-029-01 |
| https://nvd.nist.gov/vuln/detail/CVE-2026-22806 | 9,1 | vCluster Platform | Incorrect Authorization | Prior to versions 4.6.0, 4.5.4, 4.4.2, and 4.3.10 | https://github.com/loft-sh/loft/security/advisories/GHSA-c539-w4ch-7wxq |
| https://nvd.nist.gov/vuln/detail/CVE-2026-1637 | 8,8 | Tenda AC21 | Improper Restriction of Operations within the Bounds of a Memory Buffer | 16.03.08.16 | https://github.com/LX-LX88/cve/issues/25 VulDB<br>https://vuldb.com/?ctiid.343416 VulDB<br>https://vuldb.com/?id.343416 VulDB<br>https://vuldb.com/?submit.740865 VulDB<br>https://www.tenda.com.cn/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-7016 | 8,0 | Akın Software Computer Import Export Industry and Trade Ltd. QR Menu | Improper Access Control | before s1.05.12 | https://www.usom.gov.tr/bildirim/tr-26-0006 |
| https://nvd.nist.gov/vuln/detail/CVE-2026-24856 | 7,8 | iccDEV | Improper Input Validation | prior to 2.3.1.2 | https://github.com/InternationalColorConsortium/iccDEV/commit/5e53a5d25923b7794ba44e390e9b35d391f2b9c1 GitHub, Inc.<br>https://github.com/InternationalColorConsortium/iccDEV/issues/532 GitHub, Inc.<br>https://github.com/InternationalColorConsortium/iccDEV/pull/541 GitHub, Inc. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | https://github.com/InternationalColorConsortium/iccDEV/security/advisories/GHSA-w585-cv3v-c396 |
| https://nvd.nist.gov/vuln/detail/CVE-2026-22277 | **7,8** | Dell UnityVSA | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | version(s) 5.4 and prior | https://www.dell.com/support/kbdoc/en-us/000421197/dsa-2026-054-security-update-for-dell-unity-dell-unityvsa-and-dell-unity-xt-security-update-for-multiple-vulnerabilities |
| https://nvd.nist.gov/vuln/detail/CVE-2026-25116 | **7,6** | Runtipi | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | Starting in version 4.5.0 and prior to version 4.7.2 | https://github.com/runtipi/runtipi/releases/tag/v4.7.2 GitHub, Inc.<br>https://github.com/runtipi/runtipi/security/advisories/GHSA-mwg8-x997-cqw6 |
| https://nvd.nist.gov/vuln/detail/CVE-2026-1616 | **7,5** | The $uri$args | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | prior v2025.9.0 | https://github.com/RedHatProductSecurity/osim/pull/615 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-71007 | **7,5** | OneFlow | Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | v0.9.0 | https://github.com/Daisy2ang MITRE<br>https://github.com/Oneflow-Inc/oneflow/issues/10652 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-71000 | **7,5** | flow.cuda.BoolTensor component of OneFlow | Uncontrolled Resource Consumption | v0.9.0 | http://oneflow.com MITRE<br>https://github.com/Daisy2ang MITRE<br>https://github.com/Oneflow-Inc/oneflow/issues/10659 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-7713 | **7,5** | Global Interactive Design Media Software Inc. Content Management System (CMS) | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | through 21072025. | https://www.usom.gov.tr/bildirim/tr-26-0008 |
| https://nvd.nist.gov/vuln/detail/CVE-2026-1595 | **7,3** | Society Management System | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 1.0 | https://github.com/yyzq-wsx/for_cve/issues/1 VulDB<br>https://itsourcecode.com/ VulDB<br>https://vuldb.com/?ctiid.343357 VulDB<br>https://vuldb.com/?id.343357 VulDB<br>https://vuldb.com/?submit.740692 |
| https://nvd.nist.gov/vuln/detail/CVE-2026-1535 | **7,3** | Online Music Site | Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | 1.0 | https://code-projects.org/ VulDB<br>https://github.com/yuji0903/silver-guide/issues/4 VulDB<br>https://vuldb.com/?ctiid.343221 VulDB<br>https://vuldb.com/?id.343221 VulDB<br>https://vuldb.com/?submit.738706 |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| https://nvd.nist.gov/vuln/detail/CVE-2026-23896 | **7,2** | immich | Improper Privilege Management | Prior to version 2.5.0 | https://github.com/immich-app/immich/security/advisories/GHSA-237r-x578-h5mv |
| https://nvd.nist.gov/vuln/detail/CVE-2026-1400 | **7,2** | The AI Engine – The Chatbot and AI Framework for WordPress plugin for WordPress | Unrestricted Upload of File with Dangerous Type | up to, and including, 3.3.2. | https://plugins.trac.wordpress.org/browser/ai-engine/tags/3.3.0/classes/rest.php#L1104 Wordfence<br>https://plugins.trac.wordpress.org/browser/ai-engine/tags/3.3.0/classes/rest.php#L1141 Wordfence<br>https://plugins.trac.wordpress.org/changeset/3447500/ai-engine/trunk/classes/rest.php Wordfence<br>https://www.wordfence.com/threat-intel/vulnerabilities/id/d5227269-4406-4fcf-af37-f1db0af857d6?source=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2026-24902 | **7,1** | TrustTunnel | Server-Side Request Forgery (SSRF) | prior to 0.9.114 | https://github.com/TrustTunnel/TrustTunnel/commit/734bb5cf103b72390a95c853cbf91e699cc01bc0 GitHub, Inc.<br>https://github.com/TrustTunnel/TrustTunnel/security/advisories/GHSA-hgr9-frvw-5r76 |
| https://nvd.nist.gov/vuln/detail/CVE-2026-25126 | **7,1** | PolarLearn | Improper Input Validation | Prior to version 0-PRERELEASE-15 | https://github.com/polarnl/PolarLearn/commit/e6227d94d0e53e854f6a46480db8cd1051184d41 GitHub, Inc.<br>https://github.com/polarnl/PolarLearn/security/advisories/GHSA-ghpx-5w2p-p3qp |

## 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 Guidance to Address Ongoing Exploitation of Authentication Bypass Vulnerability CVE-2026-24858** | • CVE-2026-24858<br>• CVE-2025-59718<br>• CVE-2025-59719<br>• [2] CVE-2025-59718<br>• CVE-2025-59719 | **https://www.cisa.gov/news-events/alerts/2026/01/28/fortinet-releases-guidance-address-ongoing-exploitation-authentication-bypass-vulnerability-cve-2026** |
| **CISA Adds One Known Exploited Vulnerability to Catalog** | ▪ CVE-2026-1281 **Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability** | https://www.cisa.gov/news-events/alerts/2026/01/29/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 |
|---|---|
| **CISA Chief Uploaded Sensitive Documents into Public ChatGPT** | https://cybersecuritynews.com/cisa-chief-chatgpt/ |
| **Chinese APTs Hacking Asian Orgs With High-End Malware** | https://www.darkreading.com/cyberattacks-data-breaches/chinese-apts-asian-orgs-high-end-malware |

## 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 |
|---|---|
| **Russian security systems firm Delta hit by cyberattack, services disrupted** | https://therecord.media/russia-delta-security-alarm-company-cyberattack?&web_view=true |
| **Nike investigates data breach after extortion gang leaks files** | https://www.bleepingcomputer.com/news/security/nike-investigates-data-breach-after-extortion-gang-leaks-files/?&web_view=true |
| **SoundCloud Data Breach Exposes 29.8 Million Personal users Details** | https://cybersecuritynews.com/soundcloud-breach-exposes-users-details/ |
| **16 Malicious Chrome Extensions as ChatGPT Enhancements Steals ChatGPT Logins** | https://cybersecuritynews.com/16-malicious-chrome-extensions-as-chatgpt-enhancements/ |
| **MongoDB Ransomware Is Still Actively Hitting Exposed Databases** | https://www.esecurityplanet.com/threats/mongodb-ransomware-is-still-actively-hitting-exposed-databases/?&web_view=true |
| **eScan confirms update server breached to push malicious update** | https://www.bleepingcomputer.com/news/security/escan-confirms-update-server-breached-to-push-malicious-update/?&web_view=true |
| **Exposed Open Directory Leaks BYOB Framework Across Windows, Linux, and macOS** | https://cybersecuritynews.com/exposed-open-directory-leaks-byob-framework/ |
| **31.4 Tbps DDoS Attack Via Aisuru Botnet Breaks Internet With New World Record** | https://cybersecuritynews.com/31-4-tbps-ddos-attack/ |

## 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 |
|---|---|
| Two High-Severity n8n Flaws Allow Authenticated Remote Code Execution | https://thehackernews.com/2026/01/two-high-severity-n8n-flaws-allow.html |
| **APTs, Cybercriminals Widely Exploiting WinRAR Vulnerability** | https://www.securityweek.com/apts-cybercriminals-widely-exploiting-winrar-vulnerability/ |
| **Autonomous System Uncovers Long-Standing OpenSSL Flaws** | https://www.infosecurity-magazine.com/news/12-openssl-flaws/ |
| **TP-Link Archer Vulnerability Let Attackers Take Control Over the Router** | https://cybersecuritynews.com/tp-link-archer-vulnerability/ |
| **Gemini MCP Tool 0-day Vulnerability Allows Remote Attackers to Execute Arbitrary Code** | https://cybersecuritynews.com/gemini-mcp-tool-0-day-vulnerability/ |
| **ZAP JavaScript Engine Memory Leak Issue Impacts Active Scan Usage** | https://cybersecuritynews.com/zap-memory-leak-issue/ |
| **Check Point Harmony SASE Windows Client Vulnerability Enables Privilege Escalation** | https://cybersecuritynews.com/check-point-harmony-windows-client-vulnerability/ |
| **Critical Solarwinds Web Vulnerability Allows Remote Code Execution and Security Bypass** | https://cybersecuritynews.com/solarwinds-web-rce-vulnerability/ |
| SmarterMail Fixes Critical Unauthenticated RCE Flaw with CVSS 9.3 Score | https://thehackernews.com/2026/01/smartermail-fixes-critical.html |
| **3,280,081 Fortinet Devices Online With Exposed Web Properties Under Risk** | https://cybersecuritynews.com/fortinet-devices-exposed-web-properties/ |
| **Wireshark 4.6.3 Released With Vulnerabilities Dissector and Parser Crash** | https://cybersecuritynews.com/wireshark-4-6-3-released/ |

## 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 |
|---|---|
| **Fortinet Patches Exploited FortiCloud SSO Authentication Bypass** | https://www.securityweek.com/fortinet-patches-exploited-forticloud-sso-authentication-bypass/ |
| **Chrome Security Update Patches Background Fetch API Vulnerability** | https://cybersecuritynews.com/chrome-fetch-api-vulnerability/ |
| **Microsoft Releases Update for Windows 11, version 25H2 and 24H2 Systems** | https://cybersecuritynews.com/microsoft-windows-11-updates/ |

## 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 |
|---|---|
| **China-Backed 'PeckBirdy' Takes Flight for Cross-Platform Attacks** | https://www.darkreading.com/threat-intelligence/china-backed-peckbirdy-cross-platform-attacks |
| **Researchers Uncover 454,000+ Malicious Open Source Packages** | **https://www.infosecurity-magazine.com/news/454000-malicious-open-source/** |
| **Emojis in PureRAT’s Code Point to AI-Generated Malware Campaign** | https://www.infosecurity-magazine.com/news/emojis-in-purerats-code/ |
| **Swarmer Tool Evading EDR With a Stealthy Modification on Windows Registry for Persistence** | https://cybersecuritynews.com/swarmer-tool-evading-edr/ |
| **Threat Actors Leverage Real Enterprise Email Threads to Deliver Phishing Links** | https://cybersecuritynews.com/enterprise-email-threads-leveraged/ |
| **New Semantic Chaining Jailbreak Attack Bypasses Grok 4 and Gemini Nano Security Filters** | https://cybersecuritynews.com/semantic-chaining-jailbreak-attack/ |
| **Fake CAPTCHA Attack Leverages Microsoft Application Virtualization (App-V) to Deploy Malware** | https://cybersecuritynews.com/fake-captcha-attack-leverages-microsoft-application-virtualization/ |
| **HoneyMyte Hacker Group Updates CoolClient Malware to Deploy Browser Login Data Stealer** | https://cybersecuritynews.com/honeymyte-hacker-group-updates-coolclient-malware/ |
| **Hackers Weaponized Open VSX Extension with Sophisticated Malware After Reaching 5066 Downloads** | https://cybersecuritynews.com/hackers-weaponized-open-vsx-extension/ |
| **Python-based PyRAT with Cross-Platform Capabilities and Extensive Remote Access Features** | https://cybersecuritynews.com/python-based-pyrat-with-cross-platform-capabilities/ |
| **Matanbuchus Malware Downloader Evading AV Detections by Changing Components** | https://cybersecuritynews.com/matanbuchus-malware-downloader-evading-av-detections/ |
| **TA584 Actors Leveraging ClickFix Social Engineering to Deliver Tsundere Bot Malware** | https://cybersecuritynews.com/ta584-actors-leveraging-clickfix-social-engineering/ |

## 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/ |
| **15 Best Remote Monitoring Tools – 2025** | https://cybersecuritynews.com/best-remote-monitoring-tools/ |
| **Top 10 Best Exposure Management Tools In 2026** | https://cybersecuritynews.com/best-exposure-management-tools/ |
| **NETREAPER Offensive Security Toolkit That Wraps 70+ Penetration Testing Tools** | https://cybersecuritynews.com/netreaper-offensive-security-toolkit/ |

## 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/<br>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<br>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<br>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/ |