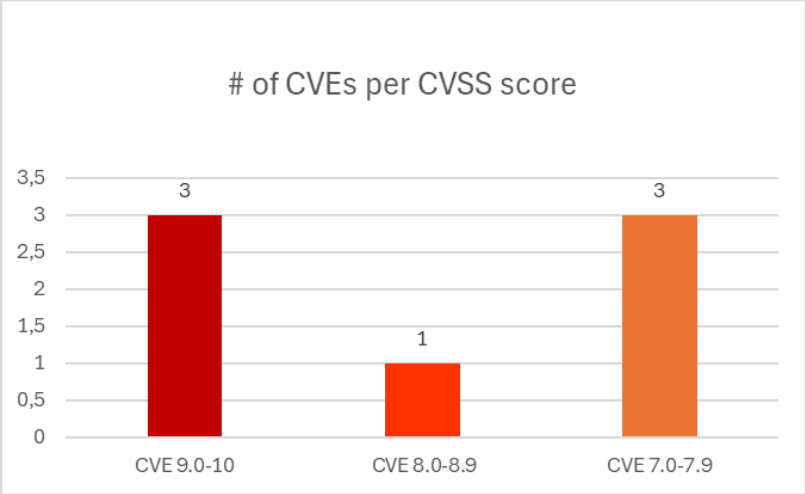
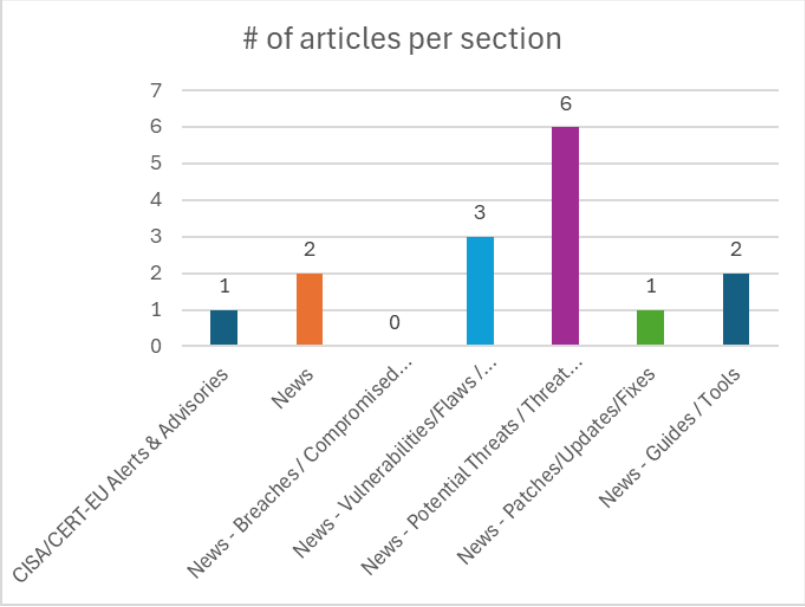

Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

**Date: 01/01/2026 - 02/01/2026**



# 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) | CVSSv3 | Προϊόν/Υπηρεσία | Τύπος Ευπάθειας | Συσκευές/Εκδόσεις που επηρεάζονται | URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης |
|---|---|---|---|---|---|
| https://nvd.nist.gov/vuln/detail/CVE-2025-14998 | 9,8 | Branda plugin for WordPress | Authorization Bypass Through User-Controlled Key | in all versions up to, and including, 3.4.24 | https://plugins.trac.wordpress.org/browser/branda-white-labeling/tags/3.4.24/inc/modules/login-screen/signup-password.php#L24<br>https://plugins.trac.wordpress.org/changeset/3429115/branda-white-labeling#file1749<br>https://www.wordfence.com/threat-intel/vulnerabilities/id/ae46be82-570f-4172-9c3f-746b894b84b9?source=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2025-66398 | 9,6 | Signal K Server | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | Versions prior to 2.19.0 | https://github.com/SignalK/signalk-server/releases/tag/v2.19.0<br>https://github.com/SignalK/signalk-server/security/advisories/GHSA-w3x5-7c4c-66p9 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-68620 | 9,1 | Signal K Server | Authentication Bypass Using an Alternate Path or Channel | Versions prior to 2.19.0 | https://github.com/SignalK/signalk-server/releases/tag/v2.19.0<br>https://github.com/SignalK/signalk-server/security/advisories/GHSA-fq56-hvg6-wvm5 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-15431 | 8,8 | UTT 进取 | Improper Restriction of Operations within the Bounds of a Memory Buffer | 512W 1.7.7-171114 | https://github.com/GUOTINGTING2297/cve/blob/main/1234/21.md<br>https://github.com/GUOTINGTING2297/cve/blob/main/1234/21.md#poc<br>https://vuldb.com/?ctiid.339353<br>https://vuldb.com/?id.339353<br>https://vuldb.com/?submit.721889 |

| | | | | | |
|---|---|---|---|---|---|
| https://nvd.nist.gov/vuln/detail/CVE-2025-68272 | 7,5 | Signal K Server | Uncontrolled Resource Consumption | Versions prior to 2.19.0 | https://github.com/SignalK/signalk-server/releases/tag/v2.19.0<br>https://github.com/SignalK/signalk-server/security/advisories/GHSA-7rqc-ff8m-7j23 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-15426 | 7,3 | jackying H-ui.admin | Improper Access Control | up to 3.1 | https://github.com/TiKi-r/CVE-Report/blob/main/H-ui.admin%20RCE.md<br>https://github.com/TiKi-r/CVE-Report/blob/main/H-ui.admin%20RCE.md#4-proof-of-concept-poc<br>https://vuldb.com/?ctiid.339348<br>https://vuldb.com/?id.339348<br>https://vuldb.com/?submit.721457 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-15427 | 7,3 | Seeyon Zhiyuan OA Web Application System | Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | up to 20251222 | https://github.com/cly-yuxiu/CVE/issues/2<br>https://vuldb.com/?ctiid.339349<br>https://vuldb.com/?id.339349<br>https://vuldb.com/?submit.721493 |

## 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 Two Industrial Control Systems Advisories** | ▪ ICSA-25-364-01: WHILL C2 Wheelchairs<br>▪ ICSA-25-345-03: AzeoTech DAQFactory (Update A) | https://www.cisa.gov/news-events/alerts/2025/12/30/cisa-releases-two-industrial-control-systems-advisories |

## 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 |
|---|---|
| **Two U.S. CyberSecurity Pros Plead Guilty for Working as ALPHV/BlackCat Affiliates** | https://cybersecuritynews.com/u-s-cybersecurity-pros-plead-guilty-as-alphv-blackcat-affiliates/ |
| **Top 10 High-Risk Vulnerabilities Of 2025 that Exploited in the Wild** | https://cybersecuritynews.com/10-high-risk-vulnerabilities-of-2025/ |

## 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 |
|---|---|
| **Apache NuttX Vulnerability Let Attackers to Crash Systems** | https://cybersecuritynews.com/apache-nuttx-vulnerability/ |
| **Critical IBM API Connect Vulnerability Let Attackers Bypass Logins** | https://cybersecuritynews.com/ibm-api-connect-vulnerability/ |
| **Critical Apache StreamPipes Vulnerability Let Attackers Seize Admin Control** | https://cybersecuritynews.com/apache-streampipes-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 |
|---|---|
| **Open-Source C2 Platform AdaptixC2 Released With Enhanced Stability, Performance, and Speed** | https://cybersecuritynews.com/adaptixc2-released/ |

## 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 |
|---|---|
| **Self-Propagating GlassWorm Weaponizing VS Code Extensions to Attack macOS Users** | https://cybersecuritynews.com/self-propagating-glassworm-weaponizing-vs-code/ |
| **New Cybercrime Tool ErrTraffic Let Attackers Automate ClickFix Attacks** | https://cybersecuritynews.com/new-cybercrime-tool-errtraffic/ |
| **DarkSpectre Hackers Infected 8.8 Million Chrome, Edge, and Firefox Users with Malware** | https://cybersecuritynews.com/darkspectre-hackers-infected-8-8-million-chrome-users/ |
| **Threat Actors Manipulating LLMs for Automated Vulnerability Exploitation** | https://cybersecuritynews.com/threat-actors-manipulating-llms/ |
| **APT36 Malware Campaign Targeting Windows LNK Files to Attack Indian Govern-ment Entities** | https://cybersecuritynews.com/apt36-malware-campaign-targeting-windows-lnk-files/ |
| **Threat Actors Advertising AI-Enhanced Metamorphic Crypter with Claims of Win-dows Defender Bypass** | https://cybersecuritynews.com/threat-actors-advertising-ai-enhanced-metamorphic-crypter/ |

## 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 |
|---|---|
| **WhatsApp Crypt Tool to Encrypt and Decrypt WhatsApp Backups** | https://cybersecuritynews.com/whatsapp-crypt-tool/ |
| **NeuroSploitv2 – AI-Powered Pentesting Tool With Claude, GPT, and Gemini mod-els to Detect vulnerabilities** | https://cybersecuritynews.com/neurosploitv2-pentesting-tool/ |

# 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/ |