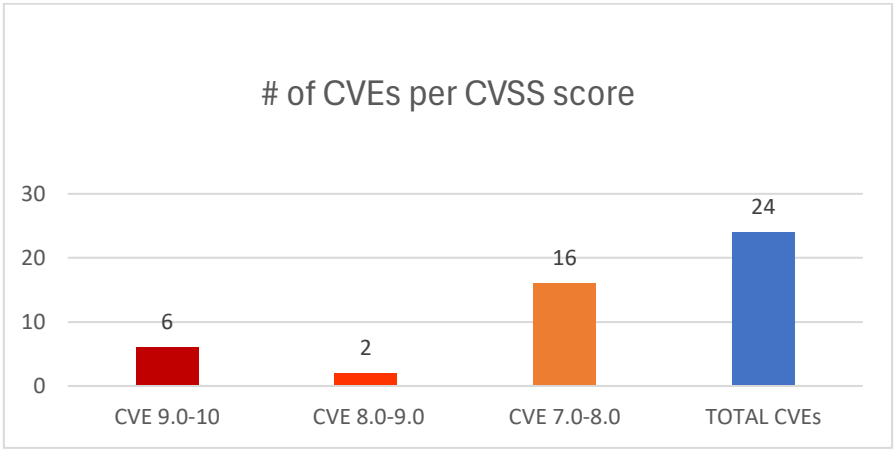
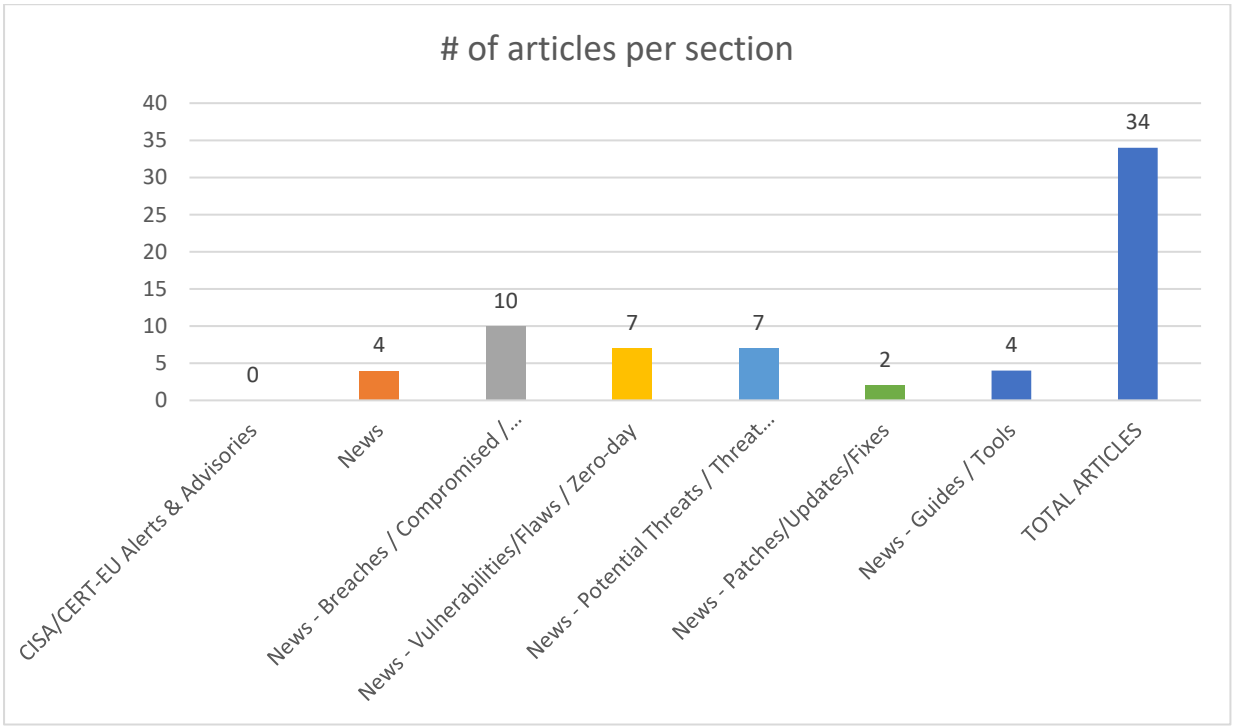

Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

**Date: 13/09/2025 - 16/09/2025**



# Contents

## Common Vulnerabilities and Exposures (CVEs)

| 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-2025-59361 | 9,8 | Chaos Controller Manager | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | | https://github.com/chaos-mesh/chaos-mesh/pull/4702 JFrog https://jfrog.com/blog/chaotic-deputy-critical-vulnerabilities-in-chaos-mesh-lead-to-kubernetes-cluster-takeover |
| https://nvd.nist.gov/vuln/detail/CVE-2025-57174 | 9,8 | Siklu Communications Etherhaul | Use of Hard-coded Cryptographic Key | 8010TX and 1200FX devices, Firmware 7.4.0 through 10.7.3 | http://ceragon.com MITRE http://etherhaul.com MITRE https://semaja2.net/2025/08/02/siklu-eh-unauthenticated-rce/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-52053 | 9,8 | TOTOLINK | Improper Neutralization of Special Elements used in a Command ('Command Injection') | X6000R V9.4.0cu.1360_B20241207 | https://github.com/w0rkd4tt/Totolink/blob/main/CVE-2025-52053/CVE-2025-52053.md MITRE https://totolink.net |
| https://nvd.nist.gov/vuln/detail/CVE-2025-10452 | 9,8 | Statistical Database System developed by Gotac | Missing Authentication for Critical Function | | https://www.twcert.org.tw/en/cp-139-10380-1ce73-2.html TWCERT/CC https://www.twcert.org.tw/tw/cp-132-10379-70d40-1.html |
| https://nvd.nist.gov/vuln/detail/CVE-2025-10432 | 9,8 | Tenda | Stack-based Buffer Overflow | AC1206 15.03.06.23 | https://github.com/M4st3rYi/IoT-VulPocs/blob/main/Tenda/AC1206/fromAdvSetMacMtuWan.md VulDB https://vuldb.com/?ctiid.323866 VulDB https://vuldb.com/?id.323866 VulDB https://vuldb.com/?submit.647527 VulDB https://www.tenda.com.cn/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-10392 | 9,8 | Mercury KM08-708H | Stack-based Buffer Overflow | GiGA WiFi Wave2 1.1.14 | https://github.com/mohdkey/IOT-CVE/blob/main/KT_GIGA_WIFI-Wave%202%20has%20a%20stack%20overflow%20vulnerability.pdf VulDB https://vuldb.com/?ctiid.323827 VulDB https://vuldb.com/?id.323827 VulDB https://vuldb.com/?submit.644596 |

| | | | | | |
|---|---|---|---|---|---|
| https://nvd.nist.gov/vuln/detail/CVE-2025-50944 | 8,8 | push.lite.avtech.com.MySSLSocketFactoryNew.checkServerTrusted | Improper Certificate Validation | AVTECH EagleEyes 2.0.0 | https://github.com/shinyColumn/CVE-2025-50944 MITRE https://shinycolumn.notion.site/eagleeyes-lite |
| https://nvd.nist.gov/vuln/detail/CVE-2025-59332 | 8,6 | 3DAlloy is a light-Weight 3D-viewer for MediaWiki | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | From 1.0 through 1.8 | https://github.com/dolfinus/3DAlloy/commit/9fac7936254886265ac89c8824c4816d009b7a1b GitHub, Inc. https://github.com/dolfinus/3DAlloy/security/advisories/GHSA-f2rp-232x-mqrh |
| https://nvd.nist.gov/vuln/detail/CVE-2025-10491 | 7,8 | MongoDB Windows | Improper Access Control | v6.0 version prior to 6.0.25, MongoDB Server v7.0 version prior to 7.0.21 and MongoDB Server v8.0 version prior to 8.0.5 | https://jira.mongodb.org/browse/SERVER-51366 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-59363 | 7,7 | One Identity OneLogin | Incorrect Resource Transfer Between Spheres | before 2025.3.0 | https://onelogin.service-now.com/support?id=kb_article&sys_id=b0aad1e11bd3ea109a47ec29b04bcb72&kb_category=a0d76d70db185340d5505eea4b96199f |
| https://nvd.nist.gov/vuln/detail/CVE-2025-9072 | 7,6 | Mattermost | URL Redirection to Untrusted Site ('Open Redirect') | versions 10.10.x <= 10.10.1, 10.5.x <= 10.5.9, 10.9.x <= 10.9.4 | https://mattermost.com/security-updates |
| https://nvd.nist.gov/vuln/detail/CVE-2025-57248 | 7,3 | SumatraPDF | NULL Pointer Dereference | 3.5.2 | https://github.com/sumatrapdfreader/sumatrapdf/issues/5035 |

| | | | | | |
|---|---|---|---|---|---|
| https://nvd.nist.gov/vuln/detail/CVE-2025-56710 | 7,3 | Profile Page of the PHPGurukul Student-Result-Management-System-Using-PHP | Cross-Site Request Forgery (CSRF) | V2.0 | https://medium.com/@mrshaikh841/csrf-pocs-1c96d9305298 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-3025 | 7,3 | Gen Digital CCleaner | Files or Directories Accessible to External Parties | 6.33.11465 on Windows | https://www.gendigital.com/us/en/contact-us/security-advisories/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-10482 | 7,3 | SourceCodester Online Student File Management System | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 1.0 | https://github.com/qcycop0101-hash/CVE/issues/11 VulDB<br>https://vuldb.com/?ctiid.323917 VulDB<br>https://vuldb.com/?id.323917 VulDB<br>https://vuldb.com/?submit.648580 VulDB<br>https://www.sourcecodester.com/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-10459 | 7,3 | PHPGurukul Beauty Parlour Management System | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 1.1 | https://github.com/xiaoxinkaishi/cve/issues/5 VulDB<br>https://phpgurukul.com/ VulDB<br>https://vuldb.com/?ctiid.323887 VulDB<br>https://vuldb.com/?id.323887 VulDB<br>https://vuldb.com/?submit.648355 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-10448 | 7,3 | Campcodes Online Job Finder System | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 1.0 | https://github.com/HAO-RAY/HCR-CVE/issues/7 VulDB<br>https://vuldb.com/?ctiid.323882 VulDB<br>https://vuldb.com/?id.323882 VulDB<br>https://vuldb.com/?submit.648023 VulDB<br>https://www.campcodes.com/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-10424 | 7,3 | 1000projects Online Student Project Report Submission and Evaluation System | Improper Access Control | 1.0 | https://github.com/lan041221/cvec/issues/22 VulDB<br>https://vuldb.com/?ctiid.323858 VulDB<br>https://vuldb.com/?id.323858 VulDB<br>https://vuldb.com/?submit.647173 VulDB<br>https://vuldb.com/?submit.647176 |
| https://nvd.nist.gov/vuln/d | 7,3 | Online Laundry Management System | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 1.0 | https://github.com/HAO-RAY/HCR-CVE/issues/3 VulDB<br>https://itsourcecode.com/ VulDB<br>https://vuldb.com/?ctiid.323860 VulDB |

| | | | | | |
|---|---|---|---|---|---|
| etail/CVE-2025-10426 | | | | | https://vuldb.com/?id.323860 VulDB<br>https://vuldb.com/?submit.647210 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-10405 | 7,3 | Baptism Information Management System | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 1.0 | https://github.com/peri0d/my_cve/issues/4 VulDB<br>https://itsourcecode.com/ VulDB<br>https://vuldb.com/?ctiid.323840 VulDB<br>https://vuldb.com/?id.323840 VulDB<br>https://vuldb.com/?submit.646904 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-10396 | 7,3 | SourceCodester Pet Grooming Management Software | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 1.0 | https://github.com/zhe293/src2/blob/master/report.md VulDB<br>https://vuldb.com/?ctiid.323831 VulDB<br>https://vuldb.com/?id.323831 VulDB<br>https://vuldb.com/?submit.645803 VulDB<br>https://www.sourcecodester.com/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-10374 | 7,3 | Shenzhen Sixun Business Management System | Improper Authorization | | https://vuldb.com/?ctiid.323788 VulDB<br>https://vuldb.com/?id.323788 VulDB<br>https://vuldb.com/?submit.639092 VulDB<br>https://www.yuque.com/hongzh0/tx13c7/lgb05p6ar7ybugcz |
| https://nvd.nist.gov/vuln/detail/CVE-2025-10371 | 7,3 | eCharge Hardy Barth Salia PLCC | Improper Access Control | 2.2.0 | https://github.com/YZS17/CVE/blob/main/Salia_PLCC/file-write-api.php.md VulDB<br>https://github.com/YZS17/CVE/blob/main/Salia_PLCC/file-write-api.php.md#poc VulDB<br>https://vuldb.com/?ctiid.323779 VulDB<br>https://vuldb.com/?id.323779 VulDB<br>https://vuldb.com/?submit.643535 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-10359 | 7,3 | Wavlink WL-WN578W2 221110 | Improper Neutralization of Special Elements used in a Command ('Command Injection') | Wavlink WL-WN578W2 221110 | https://github.com/ZZ2266/.github.io/blob/main/WAVLINK/WL-WN578W2/wireless.cgi/add_mac/ VulDB<br>https://github.com/ZZ2266/.github.io/tree/main/WAVLINK/WL-WN578W2/wireless.cgi/add_mac#proof-of-concept-poc VulDB<br>https://vuldb.com/?ctiid.323773 VulDB<br>https://vuldb.com/?id.323773 VulDB<br>https://vuldb.com/?submit.643444 |

# Τεχνική Αναφορά Κυβερνοασφάλειας: Ευπάθειες και Συμβάντα (13–16 Σεπτεμβρίου 2025)

Η τρέχουσα περίοδος χαρακτηρίζεται από ιδιαίτερη ένταση στον χώρο της κυβερνοασφάλειας, με την εμφάνιση πολλαπλών ευπαθειών υψηλής κρισιμότητας και την εκδήλωση στοχευμένων επιθέσεων μεγάλης κλίμακας. Οι καταγεγραμμένες ευπάθειες περιλαμβάνουν πολλές περιπτώσεις με βαθμολογία CVSSv3 9.8, αποκαλύπτοντας σοβαρές αδυναμίες σε κρίσιμα συστήματα και πλατφόρμες που βρίσκονται στον πυρήνα σύγχρονων υποδομών IT.

Ιδιαίτερη ανησυχία προκαλεί η ευπάθεια με κωδικό **CVE-2025-59361** στο Chaos Mesh, η οποία επιτρέπει απομακρυσμένη εκτέλεση εντολών μέσω injection σε Kubernetes clusters. Η σημασία της είναι θεμελιώδης, καθώς το Kubernetes αποτελεί βασικό συστατικό των cloud-native υποδομών και η εκμετάλλευση αυτής της ευπάθειας μπορεί να οδηγήσει σε πλήρη έλεγχο των clusters, με συνέπεια πιθανή διαρροή δεδομένων, lateral movement και εγκατάσταση persistence από επιτιθέμενους.

Παράλληλα, η ευπάθεια **CVE-2025-57174** που εντοπίζεται σε backhaul ραδιοσυσκευές Etherhaul της Siklu καταδεικνύει την επικινδυνότητα της ύπαρξης hardcoded cryptographic keys. Τα συγκεκριμένα συστήματα χρησιμοποιούνται συχνά από παρόχους δικτύων και σε υποδομές δημόσιας χρήσης, γεγονός που ενισχύει τη σημασία της γρήγορης αντιμετώπισης αυτής της αδυναμίας για την αποτροπή πιθανής παρακολούθησης ή αλλοίωσης κυκλοφορίας δεδομένων.

Ακόμη, ευπάθειες όπως η **CVE-2025-10452**, η οποία αφορά βάση δεδομένων της Gotac και επιτρέπει την πρόσβαση σε κρίσιμες λειτουργίες χωρίς καμία μορφή αυθεντικοποίησης, ενισχύουν την ανάγκη για αυστηρότερη εφαρμογή authentication/authorization μηχανισμών σε οργανισμούς που διαχειρίζονται ευαίσθητα δεδομένα.

Αν και η ευπάθεια **CVE-2025-10491** που επηρεάζει την MongoDB σε Windows έχει χαμηλότερη βαθμολογία CVSSv3 (7.8), ενδέχεται να είναι ιδιαίτερα κρίσιμη λόγω της ευρείας χρήσης της συγκεκριμένης βάσης δεδομένων σε επιχειρησιακά περιβάλλοντα παγκοσμίως. Το πρόβλημα αφορά **ανεπαρκή έλεγχο πρόσβασης**, το οποίο σε περιπτώσεις λάθους παραμετροποίησης μπορεί να επιτρέψει σε μη εξουσιοδοτημένους χρήστες την προβολή ή ακόμη και την τροποποίηση δεδομένων. Δεδομένου ότι η MongoDB χρησιμοποιείται εκτενώς σε SaaS εφαρμογές, APIs και cloud deployments, η πιθανότητα κατάχρησης αυτής της ευπάθειας αποκτά ιδιαίτερη σημασία σε όρους επιπτώσεων.

Παράλληλα με τις τεχνικές ευπάθειες, η περίοδος χαρακτηρίστηκε από σοβαρά περιστατικά ασφάλειας. Το botnet AISURU, που αξιοποίησε πάνω από 300.000 παραβιασμένους routers για να εκτελέσει επίθεση DDoS μεγέθους 11.5 Tbps, αποτελεί απόδειξη ότι οι οικιακές και μικρομεσαίες συσκευές δικτύωσης παραμένουν σημαντικό τρωτό σημείο για μαζικές επιθέσεις, οι οποίες μπορούν να πλήξουν ακόμα και μεγάλους παρόχους ή κρίσιμες υποδομές δικτύων.

Στο ίδιο πλαίσιο, η ευρεία παραβίαση του οικοσυστήματος της NPM, με επιθέσεις σε αποθετήρια όπως το ctrl/tinycolor και άλλες 40 βιβλιοθήκες με εκατομμύρια λήψεις, αποκαλύπτει τη συνεχιζόμενη αδυναμία ελέγχου της εφοδιαστικής αλυσίδας λογισμικού. Οι επιτιθέμενοι εκμεταλλεύονται τη δυσκολία εντοπισμού ύποπτων εξαρτήσεων σε έργα open source και εισάγουν κακόβουλο κώδικα ο οποίος, μέσω CI/CD pipelines, μπορεί να φτάσει απευθείας σε παραγωγικά περιβάλλοντα.

Παράλληλα, σημειώθηκε η μεγαλύτερη μέχρι στιγμής διαρροή δεδομένων από το Great Firewall της Κίνας, με 600 GB πληροφοριών να καθίστανται διαθέσιμα. Η διαρροή περιλαμβάνει metadata, αρχεία καταγραφής και πιθανώς πληροφορίες για πολιτικές πρακτικές λογοκρισίας και επιτήρησης. Οι γεωπολιτικές επιπτώσεις μιας τέτοιας παραβίασης είναι σημαντικές, ιδίως για κράτη που βασίζονται σε παρόμοιες τεχνολογίες ή συνεργάζονται με την Κίνα σε θέματα ασφάλειας και πληροφορίας.

Από τεχνικής σκοπιάς, ιδιαίτερη ανησυχία προκαλούν επιθέσεις όπως το Phoenix RowHammer, το οποίο καταφέρνει να παρακάμψει προστασίες σε DDR5 μνήμες εντός 109 δευτερολέπτων, ανοίγοντας τον δρόμο για πιθανές φυσικές επιθέσεις σε servers και κρίσιμα συστήματα. Επιπλέον, το 0-click exploit στον Linux Kernel (KSMBD), αποδεικνύει ότι ακόμα και ο open-source πυρήνας του λειτουργικού συστήματος παραμένει ευάλωτος σε πλήρως αυτοματοποιημένες επιθέσεις χωρίς καμία αλληλεπίδραση χρήστη, γεγονός που εγείρει ανησυχίες για embedded συστήματα και IoT υποδομές.

Οι προσπάθειες mitigation που ακολουθούν είναι εν μέρει επαρκείς. Η Apple κυκλοφόρησε αναβαθμίσεις για το iOS 26 και το macOS Tahoe 26, διορθώνοντας πάνω από 50 ευπάθειες, ενώ η Microsoft έδωσε επιδιορθώσεις για προβλήματα στο Windows 11 24H2, τα οποία όμως υποδεικνύουν deeper architectural flaws στο audio stack. Ειδικά για περιπτώσεις όπως το MongoDB (CVE-2025-10491), όπου υπήρχε ανεπαρκής έλεγχος πρόσβασης στις εκδόσεις v6 έως και v8, η επίσπευση της αναβάθμισης είναι επιτακτική για την αποτροπή παραβιάσεων σε παραγωγικά περιβάλλοντα.

Τέλος, αξιοσημείωτη είναι η αυξανόμενη χρήση εργαλείων Τεχνητής Νοημοσύνης, όχι μόνο από ερευνητές αλλά και από επιτιθέμενους. Η υποκλοπή προσωπικών δεδομένων μέσω εργαλείων όπως το ChatGPT με υποστήριξη για MCP, η δημιουργία polymorphic malware που παρακάμπτει antivirus μηχανισμούς, καθώς και η χρήση generative AI για spear phishing και επιθέσεις κοινωνικής μηχανικής, ενισχύουν την ανάγκη για νέα πρότυπα στην ανίχνευση και απόκριση απειλών.

Συνοψίζοντας, το τεχνικό περιβάλλον που διαμορφώνεται χαρακτηρίζεται από κλιμακούμενη πολυπλοκότητα, ταχύτατες εξελίξεις στον χώρο των επιθέσεων και μια εμφανή υστέρηση στην προληπτική θωράκιση κρίσιμων υποδομών. Η συνεχής επιτήρηση, η επιτάχυνση της εφαρμογής patches και η επένδυση σε τεχνολογίες behavior-based ανίχνευσης απειλών καθίστανται πλέον αναγκαίες πρακτικές, όχι επιλογές.

## CISA/CERT-EU Alerts & Advisories

| Σύντομη περιγραφή / Τίτλος | Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες | URL |
|---|---|---|
| | | |

## News

| Σύντομη περιγραφή / Τίτλος | URL |
|---|---|
| Building Resilient IT Infrastructure From the Start | https://www.darkreading.com/vulnerabilities-threats/building-resilient-it-infrastructure |
| CISA at Risk After OIG Accuses it of Wasting Federal Funds | https://www.infosecurity-magazine.com/news/cisa-oig-accuses-wasting-federal/ |
| AI-Forged Military IDs Used in North Korean Phishing Attack | https://www.infosecurity-magazine.com/news/ai-military-ids-north-korea/ |
| Pro-Russian Hackers Attacking Key Industries in Major Countries Around The World | https://cybersecuritynews.com/pro-russian-hackers-attacking-key-industries/ |

## Breaches / Compromised / Hacked

| Σύντομη περιγραφή / Τίτλος | URL |
|---|---|
| FinWise Bank Warns of Insider Data Breach | https://www.infosecurity-magazine.com/news/finwise-bank-warns-of-insider-data/ |
| AISURU Botnet With 300,000 Hijacked Routers Behind The Recent Massive 11.5 Tbps DDoS Attack | https://cybersecuritynews.com/aisuru-botnet-with-300000-hijacked-routers/ |
| Hackers steal millions of Gucci, Balenciaga, and Alexander McQueen customer records | https://securityaffairs.com/182236/cyber-crime/hackers-steal-millions-of-gucci-balenciaga-and-alexander-mcqueen-customer-records.html?&web_view=true |
| West Virginia Credit Union Notifying 187,000 People Impacted by 2023 Data Breach | https://www.securityweek.com/west-virginia-credit-union-notifying-187000-people-impacted-by-2023-data-breach/?&web_view=true |
| Vietnam, Panama governments suffer incidents leaking citizen data | https://therecord.media/vietnam-cic-panama-finance-ministry-cyberattacks?&web_view=true |
| 600 GB of Alleged Great Firewall of China Data Published in Largest Leak Yet | https://hackread.com/great-firewall-of-china-data-published-largest-leak/?&web_view=true |
| Google confirms fraudulent account created in law enforcement portal | https://www.bleepingcomputer.com/news/security/google-confirms-fraudulent-account-created-in-law-enforcement-portal/?&web_view=true |
| Massive Supply Chain Attack Hijacks ctrl/tinycolor With 2 Million Downloads and Other 40 NPM Packages | https://cybersecuritynews.com/npm-supply-chain-ctrl-tinycolor/ |
| Great Firewall of China's Sensitive Data of Over 500GB+ Leaked Online | https://cybersecuritynews.com/great-firewall-of-china-sensitive-data-leaked/ |
| HybridPetya Mimics NotPetya, Adds UEFI Compromise | https://www.infosecurity-magazine.com/news/hybridpetya-mimics-notpetya-uefi/ |

## Vulnerabilities / Flaws / Zero-day

| Σύντομη περιγραφή / Τίτλος | URL |
|---|---|
| Phoenix RowHammer Attack Bypasses Advanced DDR5 Memory Protections in 109 Seconds | https://thehackernews.com/2025/09/phoenix-rowhammer-attack-bypasses.html |
| ChatGPT's New Support for MCP Tools Let Attackers Exfiltrate All Private Details From Email | https://cybersecuritynews.com/chatgpt-mcp-tools-private-data/ |
| 0-Click Linux Kernel KSMBD RCE Exploit From N-Day Vulnerabilities | https://cybersecuritynews.com/0-click-linux-kernel-ksmbd-rce-exploit/ |
| Microsoft Confirms 900+ XSS Vulnerabilities Found in IT Services, Ranging from Low Impact to Zero-Click | https://cybersecuritynews.com/microsoft-confirms-900-xss-vulnerabilities/ |
| IBM QRadar SIEM Vulnerability Let Attackers Perform Unauthorized Actions | https://cybersecuritynews.com/ibm-qradar-siem-vulnerability-unauthorized/ |
| FlowiseAI Password Reset Token Vulnerability Allows Account Takeover | https://cybersecuritynews.com/flowiseai-password-reset-token-vulnerability/ |
| BitlockMove Tool Enables Lateral Movement via Bitlocker DCOM & COM Hijacking | https://cybersecuritynews.com/bitlockmove/ |

## Patches / Updates / Fixes

| Σύντομη περιγραφή / Τίτλος | URL |
|---|---|
| Apple Rolls Out iOS 26, macOS Tahoe 26 With Patches for Over 50 Vulnerabilities | https://www.securityweek.com/apple-rolls-out-ios-26-macos-tahoe-26-with-patches-for-over-50-vulnerabilities/ |
| Microsoft Fixes Windows 11 24H2 Audio Issue that Stops Bluetooth Headsets and Speakers Working | https://cybersecuritynews.com/windows-11-24h2-audio-issue/ |

## Potential threats / Threat intelligence

| Σύντομη περιγραφή / Τίτλος | URL |
|---|---|
| FBI Warns of Threat Actors Hitting Salesforce Customers | https://www.darkreading.com/cyberattacks-data-breaches/fbi-warns-threat-actors-salesforce-customers |
| Phishing Campaigns Drop RMM Tools for Remote Access | https://www.infosecurity-magazine.com/news/phishing-campaigns-rmm-tools/ |
| Open Source CyberSOCEval Sets New Standards for AI in Malware Analysis and Threat Intelligence | https://cybersecuritynews.com/cybersoceval/ |
| New Malware Attack Leverages SVGs, Email Attachments to Deliver XWorm and Remcos RAT | https://cybersecuritynews.com/new-malware-attack-leverages-svgs/ |
| Hackers Using Generative AI 'ChatGPT' to Evade Anti-virus Defenses | https://cybersecuritynews.com/hackers-using-generative-ai-chatgpt/ |
| DarkCloud Stealer Attacking Financial Companies With Weaponized RAR Attachments | https://cybersecuritynews.com/darkcloud-stealer-attacking-financial-companies/ |
| New VoidProxy PhaaS Service Attacking Microsoft 365 and Google Accounts | https://cybersecuritynews.com/new-voidproxy-phaas-service/ |

## Guides / Tools

| 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/ |
| **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/ |

# 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/ |