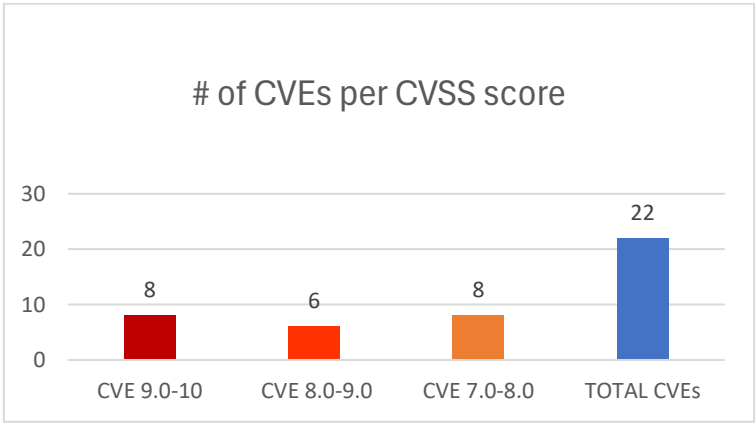
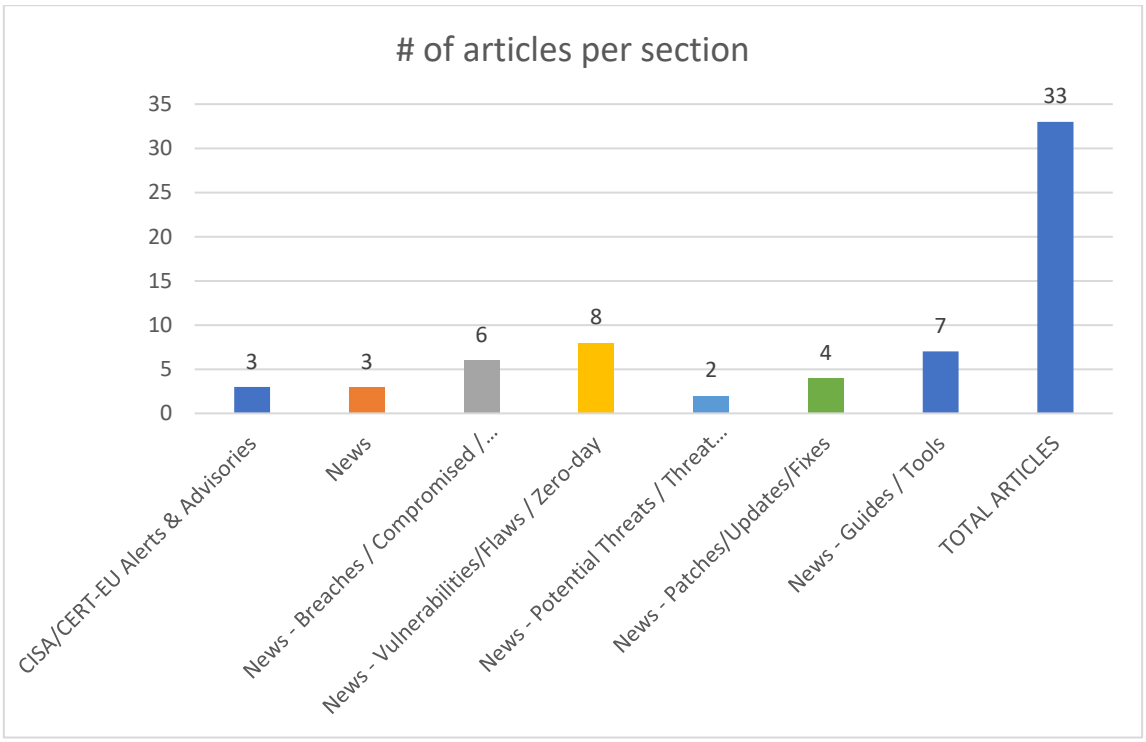

Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

**Date: 04/11/2025 - 07/11/2025**



# 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-2025-55108 | 10,0 | The Control-M/Agent | Missing Authentication for Critical Function | | https://bmcapps.my.site.com/casemgmt/sc_KnowledgeArticle?sfdcid=000441962 Airbus https://bmcapps.my.site.com/casemgmt/sc_KnowledgeArticle?sfdcid=000442099 Airbus https://bmcapps.my.site.com/casemgmt/sc_KnowledgeArticle?sfdcid=000442271 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-61956 | 10,0 | Radiometrics VizAir | Missing Authentication for Critical Function | | https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2025/icsa-25-308-04.json ICS-CERT https://www.cisa.gov/news-events/ics-advisories/icsa-25-308-04 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-63334 | 9,8 | PocketVJ CP PocketVJ-CP-v3 pvj | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 3.9.1 | https://gist.github.com/mamdouhalrekabi-ops/e7686a0bdd197c77c1b54191e1a2880f MITRE https://github.com/magdesign/PocketVJ-CP-v3/releases/tag/release |
| https://nvd.nist.gov/vuln/detail/CVE-2025-12674 | 9,8 | The KiotViet Sync plugin for WordPress | Unrestricted Upload of File with Dangerous Type | up to, and including, 1.8.5 | https://wordpress.org/plugins/kiotvietsync/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/7fdd670f-2a71-4c1d-af46-f0fd05352f7e?source=cve |

| | | | | | |
|---|---|---|---|---|---|
| https://nvd.nist.gov/vuln/detail/CVE-2025-11749 | 9,8 | The AI Engine plugin for WordPress | Exposure of Sensitive Information to an Unauthorized Actor | up to, and including, 3.1.3 | https://plugins.trac.wordpress.org/browser/ai-engine/trunk/labs/mcp.php#L226 Wordfence https://plugins.trac.wordpress.org/changeset/3380753/ai-engine#file10 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/06eaf624-aedf-453d-8457-d03a572fac0d?source=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2025-12493 | 9,8 | The ShopLentor – WooCommerce Builder for Elementor & Gutenberg +21 Modules | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | up to, and including, 3.2.5 | https://plugins.trac.wordpress.org/browser/woolentor-addons/trunk/classes/class.ajax_actions.php#L213 Wordfence https://plugins.trac.wordpress.org/browser/woolentor-addons/trunk/classes/class.ajax_actions.php#L241 Wordfence https://plugins.trac.wordpress.org/browser/woolentor-addons/trunk/classes/class.ajax_actions.php#L42 Wordfence https://plugins.trac.wordpress.org/browser/woolentor-addons/trunk/includes/addons/product-grid/base/class.product-grid-base.php#L378 Wordfence https://plugins.trac.wordpress.org/changeset/3388234/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/12bb4bb9-e908-43ad-8fb1-59418580f5e1?source=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2025-12682 | 9,8 | The Easy Upload Files During Checkout plugin for WordPress | Unrestricted Upload of File with Dangerous Type | up to, and including, 2.9.8. | https://plugins.trac.wordpress.org/changeset/3384711/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/6a050764-0ba6-49a4-bd71-f79e3129fc4c?source=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2025-63416 | 9,1 | SelfBest platform | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 2023.3 | https://rohitchaudhary045.medium.com/cve-2025-63416-the-admin-panel-heist-stored-xss-to-privilege-escalation-b4c69d8487f1 MITRE https://self.best |
| https://nvd.nist.gov/vuln/detail/CVE-2025-21078 | 8,8 | Smart Switch | | prior to version 3.7.68.6 | https://security.samsungmobile.com/serviceWeb.smsb?year=2025&month=11 |

| | | | | | |
|---|---|---|---|---|---|
| https://nvd.nist.gov/vuln/detail/CVE-2025-64109 | 8,8 | Cursor CLI Beta | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | | https://github.com/cursor/cursor/security/advisories/GHSA-4hwr-97q3-37w2 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-12384 | 8,6 | The Document Embedder – Embed PDFs, Word, Excel, and Other Files plugin for WordPress | Missing Authorization | up to, and including, 2.0.0 | https://plugins.trac.wordpress.org/changeset?old=3359820&old_path=document-emberdder%2Ftrunk%2Fdocument-library-block.php&new=&new_path=document-emberdder%2Ftrunk%2Fdocument-library-block.php Wordfence https://plugins.trac.wordpress.org/changeset?old=3359820&old_path=document-emberdder%2Ftrunk%2Fincludes%2FDocumentLibrary%2FInit-DocumentLibrary.php&new=&new_path=document-emberdder%2Ftrunk%2Fincludes%2FDocumentLibrary%2FInit-DocumentLibrary.php Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/eb7e4e96-a4ff-4c6c-91de-c0e5ba78f0da?source=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2025-23358 | 8,2 | NVIDIA NVApp for Windows | Uncontrolled Search Path Element | | https://nvd.nist.gov/vuln/detail/CVE-2025-23358 NVIDIA Corporation https://nvidia.custhelp.com/app/answers/detail/a_id/5717 NVIDIA Corporation https://www.cve.org/CVERecord?id=CVE-2025-23358 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-12497 | 8,1 | The Premium Portfolio Features for Phlox theme plugin for WordPress | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusio | up to, and including, 2.3.10 | https://plugins.trac.wordpress.org/changeset/3388727/auxin-portfolio Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/518abad2-d3cc-4d15-83d2-8fd99d30500c?source=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2025-10622 | 8,0 | Red Hat Satellite (Foreman component) | Client-Side Enforcement of | | https://access.redhat.com/errata/RHSA-2025:19721 Red Hat, Inc. https://access.redhat.com/errata/RHSA-2025:19832 Red Hat, Inc. https://access.redhat.com/errata/RHSA-2025:19855 Red Hat, Inc. https://access.redhat.com/errata/RHSA-2025:19856 Red Hat, Inc. |

| | | | | | |
|---|---|---|---|---|---|
| | | | Server-Side Security | | https://access.redhat.com/security/cve/CVE-2025-10622 Red Hat, Inc. https://bugzilla.redhat.com/show_bug.cgi?id=2396020 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-54526 | 7,8 | Fuji Electric Monitouch | Stack-based Buffer Overflow | V-SFT-6 | https://felib.fujielectric.co.jp/en/document_search?tab=software&document1%5B1%5D=M10009&document2%5B1%5D=M20104&product1%5B1%5D=P10003&product2%5B1%5D=P20023&product3%5B1%5D=P30623&product4%5B1%5D=S11133&discontinued%5B1%5D=0&count=20&sort=en_title&page=1&region=en-glb ICS-CERT https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2025/icsa-25-308-01.json ICS-CERT https://www.cisa.gov/news-events/ics-advisories/icsa-25-308-01 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-63248 | 7,5 | DWSurvey | Authorization Bypass Through User-Controlled Key | 6.14.0 | https://gitee.com/wkeyuan/DWSurvey MITRE https://github.com/Chen1-Boop/CVE/blob/main/CVE-2025-63248.md |
| https://nvd.nist.gov/vuln/detail/CVE-2025-12139 | 7,5 | The File Manager for Google Drive – Integrate Google Drive with WordPress plugin for WordPress | Exposure of Sensitive Information to an Unauthorized Actor | up to, and including, 1.5.3 | https://plugins.trac.wordpress.org/browser/integrate-google-drive/tags/1.5.3/includes/class-enqueue.php#L232 Wordfence https://plugins.trac.wordpress.org/browser/integrate-google-drive/tags/1.5.3/includes/class-enqueue.php#L243 Wordfence https://plugins.trac.wordpress.org/browser/integrate-google-drive/tags/1.5.3/includes/class-enqueue.php#L88 Wordfence https://plugins.trac.wordpress.org/changeset/3387825/integrate-google-drive Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/607073ad-3a4a-4a21-af0f-3ade81382605?source=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2025-12197 | 7,5 | The The Events Calendar plugin for WordPress | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | versions 6.15.1.1 to 6.15.9 | https://plugins.trac.wordpress.org/changeset/3386042/the-events-calendar Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/bc927a93-0cb2-4211-9f93-c0671039011e?source=cve |

| | | | | | |
|---|---|---|---|---|---|
| https://nvd.nist.gov/vuln/detail/CVE-2025-32786 | 7,5 | The GLPI Inventory Plugin | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 1.5.0 and below | https://github.com/glpi-project/glpi-inventory-plugin/blob/1.5.1/CHANGELOG.md GitHub, Inc. https://github.com/glpi-project/glpi-inventory-plugin/releases/tag/1.5.1 GitHub, Inc. https://github.com/glpi-project/glpi-inventory-plugin/security/advisories/GHSA-w2cp-r675-6xpq |
| https://nvd.nist.gov/vuln/detail/CVE-2025-54334 | 7,5 | NPU driver in Samsung Mobile Processor Exynos | NULL Pointer Dereference | 1280, 2200, 1380, 1480, 2400, 1580, 2500 | https://semiconductor.samsung.com/support/quality-support/product-security-updates/ MITRE https://semiconductor.samsung.com/support/quality-support/product-security-updates/cve-2025-54334/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-62369 | 7,2 | Xibo | Improper Control of Generation of Code ('Code Injection') | Versions 4.3.0 | https://github.com/xibosignage/xibo-cms/commit/0f4e88396111ea027785a48dd8f5eeb14536bd71 GitHub, Inc. https://github.com/xibosignage/xibo-cms/commit/ecd4f9d2cea739a46756a108a839cac80f65cf10 GitHub, Inc. https://github.com/xibosignage/xibo-cms/releases/tag/4.3.1 GitHub, Inc. https://github.com/xibosignage/xibo-cms/security/advisories/GHSA-7rmm-689c-gjgv GitHub, Inc. https://patch-diff.githubusercontent.com/raw/xibosignage/xibo-cms/pull/3128.patch |
| https://nvd.nist.gov/vuln/detail/CVE-2025-21079 | 7,1 | Samsung Members | Improper input validation | 5.5.01.3 | https://security.samsungmobile.com/serviceWeb.smsb?year=2025&month=11 |

## 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 Five Industrial Control Systems Advisories** | ▪ **ICSA-25-308-01 Fuji Electric Monitouch V-SFT-6**<br>▪ **ICSA-25-308-02 Survision License Plate Recognition Camera**<br>▪ **ICSA-25-308-03 Delta Electronics CNCSoft-G2**<br>▪ **ICSA-25-308-04 Radiometrics VizAir**<br>▪ **ICSA-25-308-05 IDIS ICM Viewer** | **https://www.cisa.gov/news-events/alerts/2025/11/04/cisa-releases-five-industrial-control-systems-advisories** |
| **CISA Adds Two Known Exploited Vulnerabilities to Catalog** | ▪ **CVE-2025-11371 Gladinet CentreStack and Triofox Files or Directories Accessible to External Parties Vulnerability**<br>▪ **CVE-2025-48703 CWP Control Web Panel OS Command Injection Vulnerability** | **https://www.cisa.gov/news-events/alerts/2025/11/04/cisa-adds-two-known-exploited-vulnerabilities-catalog** |
| **CISA Releases Four Industrial Control Systems Advisories** | ▪ ICSA-25-310-01 Advantech DeviceOn iEdge<br>▪ ICSA-25-310-02 Ubia Ubox<br>▪ ICSA-25-310-03 ABB FLXeon Controllers<br>▪ ICSA-25-282-01 Hitachi Energy Asset Suite (Update A) | https://www.cisa.gov/news-events/alerts/2025/11/06/cisa-releases-four-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 |
|---|---|
| **Kimsuky Debuts HTTPTroy Backdoor Against South Korea Users** | **https://www.darkreading.com/vulnerabilities-threats/kimsuky-httptroy-backdoor-south-korea-users** |
| **Europe Sees Increase in Ransomware, Extortion Attacks** | **https://www.darkreading.com/cyberattacks-data-breaches/europe-increase-ransomware-extortion** |
| **Google Warns of New PROMPTFLUX Malware Using Gemini API to Rewrite Its Own Source Code** | **https://cybersecuritynews.com/promptflux-malware-using-gemini-api/** |

## 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 |
|---|---|
| Hyundai AutoEver America data breach exposes SSNs, drivers licenses | https://www.bleepingcomputer.com/news/security/hyundai-autoever-america-data-breach-exposes-ssns-drivers-licenses/?&web_view=true |
| Media giant Nikkei reports data breach impacting 17,000 people | https://www.bleepingcomputer.com/news/security/media-giant-nikkei-reports-data-breach-impacting-17-000-people/?&web_view=true |
| Data breach at major Swedish software supplier impacts 1.5 million | https://www.bleepingcomputer.com/news/security/data-breach-at-major-swedish-software-supplier-impacts-15-million/?&web_view=true |
| More than $100 million stolen in exploit of Balancer DeFi protocol | https://therecord.media/crypto-heist-balancer-exploit?&web_view=true |
| AI Engine WordPress Plugin Exposes 100,000 WordPress Sites to Privilege Escalation Attacks | https://cybersecuritynews.com/ai-engine-wordpress-plugin-exposes-100000-wordpress-sites/ |
| NGate Malware Enables Unauthorized Cash Withdrawals at ATMs Using Victims' Payment Cards | https://cybersecuritynews.com/ngate-malware-enables-unauthorized-cash-withdrawals/ |

## 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 τις 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 |
|---|---|
| CISA Adds Gladinet and CWP Flaws to KEV Catalog Amid Active Exploitation Evidence | https://thehackernews.com/2025/11/cisa-adds-gladinet-and-cwp-flaws-to-kev.html |
| Researchers Find ChatGPT Vulnerabilities That Let Attackers Trick AI Into Leaking Data | https://thehackernews.com/2025/11/researchers-find-chatgpt.html |
| Google's AI 'Big Sleep' Finds 5 New Vulnerabilities in Apple's Safari WebKit | https://thehackernews.com/2025/11/googles-ai-big-sleep-finds-5-new.html |
| Exploited 'Post SMTP' Plugin Flaw Exposes WordPress Sites to Takeover | https://www.securityweek.com/exploited-post-smtp-plugin-flaw-exposes-wordpress-sites-to-takeover/ |
| Hackers exploit critical auth bypass flaw in JobMonster WordPress theme | https://www.bleepingcomputer.com/news/security/hackers-exploit-critical-auth-bypass-flaw-in-jobmonster-wordpress-theme/ |
| APT 'Bronze Butler' Exploits Zero-Day to Root Japan Orgs | https://www.darkreading.com/application-security/bronze-butler-apt-exploits-zero-day-vuln-root-japan |
| Claude Desktop Extensions Vulnerable to Web-Based Prompt Injection | https://www.infosecurity-magazine.com/news/claude-desktop-extensions-prompt/ |

| | |
|---|---|
| **Windows Cloud Files Mini Filter Driver Vulnerability Exploited to Escalate Privileges** | **https://cybersecuritynews.com/windows-cloud-files-vulnerability-exploited/** |

## 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 |
|---|---|
| **Apple Patches 19 WebKit Vulnerabilities** | **https://www.securityweek.com/apple-patches-19-webkit-vulnerabilities/** |
| **Chrome Emergency Update to Patch Multiple Vulnerabilities that Enable Remote Code Execution** | **https://cybersecuritynews.com/chrome-emergency-update/** |
| **Cisco Patches Critical Vulnerabilities in Contact Center Appliance** | https://www.securityweek.com/cisco-patches-critical-vulnerabilities-in-contact-center-appliance/ |
| **FreeBSD-based OPNsense Firewall Released for Security Issues and Improvements** | https://cybersecuritynews.com/freebsd-based-opnsense-firewall/ |

## 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 |
|---|---|
| **SesameOp Backdoor Uses OpenAI API for Covert C2** | **https://www.darkreading.com/cyberattacks-data-breaches/sesameop-backdoor-openai-api-covert-c2** |
| **APT-C-60 Attacking Job Seekers to Download Weaponized VHDX File from Google Drive to Steal Sensitive Data** | **https://cybersecuritynews.com/apt-c-60-attacking-job-seekers/** |

## 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/<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/ |