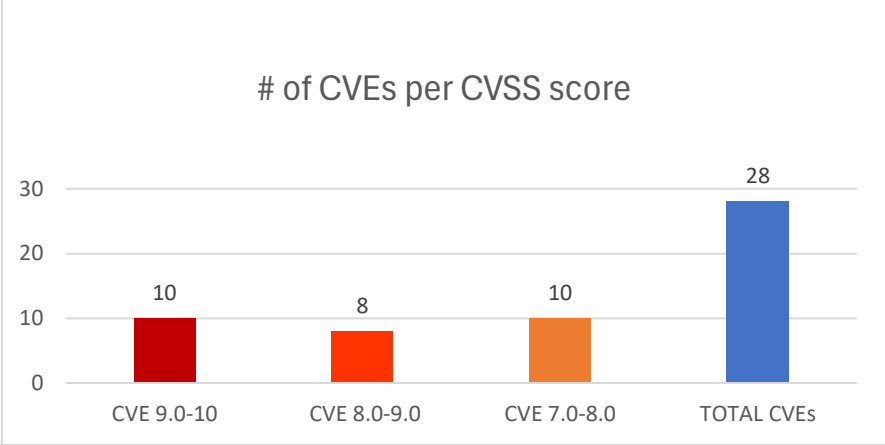
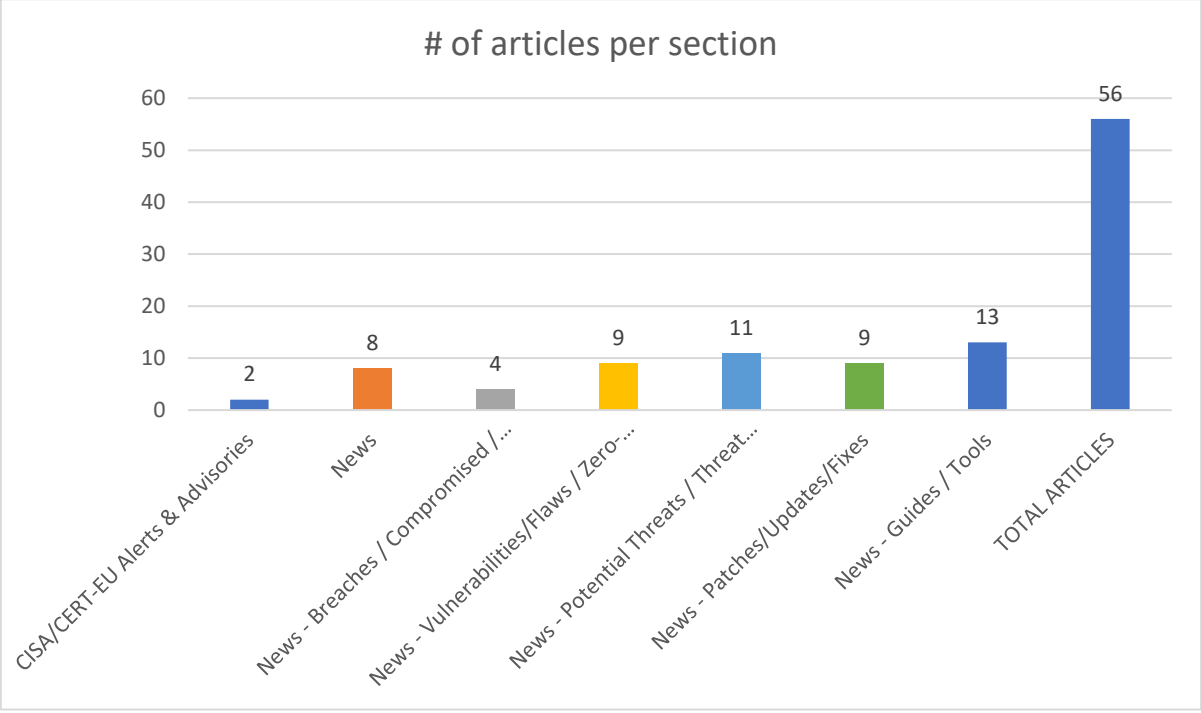

Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

**Date: 17/06/2026 - 19/06/2026**



# 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-2026-49257 | 10,0 | mcp-pinot | Missing Authentication for Critical Function | 3.0.1 and below | https://github.com/startreedata/mcp-pinot/commit/1c7d3f9cd384854bf72c127d230bdb32299475ad GitHub, Inc. https://github.com/startreedata/mcp-pinot/issues/90 GitHub, Inc. https://github.com/startreedata/mcp-pinot/pull/95 GitHub, Inc. https://github.com/startreedata/mcp-pinot/security/advisories/GHSA-73cv-556c-w3g6 |
| https://nvd.nist.gov/vuln/detail/CVE-2026-47647 | 9,9 | Microsoft Dynamics 365 | Improper Access Control | | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47647 |
| https://nvd.nist.gov/vuln/detail/CVE-2026-12183 | 9,8 | Nefteprodukttekhnika BUK TSG Gas Station Automation System | Improper Authentication | 2.9.1 through 2.10.2 | https://bukts.ru/repo-bukts-current TuranSec https://cwe.mitre.org/data/definitions/287.html TuranSec https://cwe.mitre.org/data/definitions/306.html TuranSec https://github.com/ciprobe/bukts_auth_bypass |
| https://nvd.nist.gov/vuln/detail/CVE-2026-8024 | 9,8 | ibaPDA or ibaDatCoordinator | Deserialization of Untrusted Data | | https://certvde.com/en/advisories/VDE-2026-051 CERT VDE https://iba.csaf-tp.certvde.com/.well-known/csaf/white/2026/vde-2026-051.json |
| https://nvd.nist.gov/vuln/detail/CVE-2026-47846 | 9,8 | Bitnami Cassandra | Use of Hard-coded Credentials | 4.0.x prior to 4.0.20-photon-5-r7; 4.1.x prior to 4.1.11-photon-5-r7; 5.0.x prior to | https://github.com/bitnami/containers/security/advisories/GHSA-8q3j-37vg-8fc2 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | 5.0.8-photon-5-r4 / 5.0.8-debian-12-r3 | |
| https://nvd.nist.gov/vuln/detail/CVE-2026-54390 | 9,8 | JTL Shop | Improper Neutralization of Special Elements Used in a Template Engine | 5.2.0 through 5.7.1 | https://forum.jtl-software.de/threads/jtl-shop-5-7-aktuell-5-7-2.246278/ VulnCheck https://sansec.io/research/jtl-shop-ssti-rce VulnCheck https://www.vulncheck.com/advisories/jtl-shop-server-side-template-injection-via-smarty-renderer |
| https://nvd.nist.gov/vuln/detail/CVE-2026-55740 | 9,8 | Nur-Alam39 bus-ticket | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | | https://github.com/Nur-Alam39/bus-ticket TuranSec https://github.com/Nur-Alam39/bus-ticket/blob/459cabdbeb99c00225b26e46e3c2c30ae1de7bad/bus_info.php#L14-L16 |
| https://nvd.nist.gov/vuln/detail/CVE-2026-55742 | 9,6 | Cotonti | Cross-Site Request Forgery (CSRF) | 1.0.0 | https://github.com/Cotonti/Cotonti TuranSec https://github.com/Cotonti/Cotonti/blob/f43f1fc38ba4e02027786dad9dac1435c7c52b30/system/admin/admin.rights.php#L53 |
| https://nvd.nist.gov/vuln/detail/CVE-2026-49454 | 9,1 | Relyra | Improper Authentication | 1.0.0 and 1.1.0 | https://github.com/szTheory/relyra/commit/2e456897af3158c175bb490ce7fc51d6241c8922 GitHub, Inc. https://github.com/szTheory/relyra/commit/8910200 GitHub, Inc. https://github.com/szTheory/relyra/security/advisories/GHSA-jv46-xfwm-36j7 |
| https://nvd.nist.gov/vuln/detail/CVE-2026-12045 | 9,0 | pgAdmin 4 AI Assistant | Improper Neutralization of Special Elements used in a Command ('Command Injection') | from 9.13 before 9.16 | https://github.com/pgadmin-org/pgadmin4/commit/bf4792444446f0e7ab721d23cbd6bfe6afaa7a8b PostgreSQL https://github.com/pgadmin-org/pgadmin4/issues/10022 |
| https://nvd.nist.gov/vuln/detail/CVE-2026-12174 | 8,8 | D-Link DCS-935L | Improper Restriction of Operations within the Bounds of a Memory Buffer | 1.10.01 | https://github.com/Real-Simplicity/cve-database/tree/main/CVE_Report_DLink_DCS935L_Format_String |

| | | | | | |
|---|---|---|---|---|---|
| https://nvd.nist.gov/vuln/detail/CVE-2026-12186 | 8,8 | GL.iNet GL-MT3000 | Improper Neutralization of Special Elements used in a Command ('Command Injection') | up to 4.4.5 | https://fw.gl-inet.com/firmware/mt3000/release/mt3000-4.8.1-0819-1755615825.tar VulDB https://github.com/StrTzz123/iot_vul/blob/main/GL-iNet/MT3000/4.4.5/tor_set_config/Readme.md |
| https://nvd.nist.gov/vuln/detail/CVE-2026-56078 | 8,8 | PraisonAI | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | before 1.5.115 | https://github.com/MervinPraison/PraisonAI VulnCheck https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-766v-q9x3-g744 VulnCheck https://www.vulncheck.com/advisories/praisonai-arbitrary-file-read-and-write-via-path-traversal-in-multiagentmonitor |
| https://nvd.nist.gov/vuln/detail/CVE-2026-8461 | 8,8 | FFmpeg's libavcodec library | Out-of-bounds Write | before version 8.1.2 | https://code.ffmpeg.org/FFmpeg/FFmpeg/pulls/23159 |
| https://nvd.nist.gov/vuln/detail/CVE-2026-54420 | 8,5 | LiteSpeed cPanel plugin | UNIX Symbolic Link (Symlink) Following | before 2.4.8 | https://blog.litespeedtech.com/2026/06/01/security-update-for-litespeed-cpanel-plugin-2/ MITRE https://www.litespeedtech.com/products/litespeed-web-server/control-panel-support/cpanel |
| https://nvd.nist.gov/vuln/detail/CVE-2026-54412 | 8,2 | LiamBindle MQTT-C | Out-of-bounds Read | through version 1.1.6 | https://cwe.mitre.org/data/definitions/125.html TuranSec https://cwe.mitre.org/data/definitions/191.html TuranSec https://github.com/LiamBindle/MQTT-C TuranSec https://github.com/LiamBindle/MQTT-C/blob/v1.1.6/src/mqtt.c#L1334 |
| https://nvd.nist.gov/vuln/detail/CVE-2026-56020 | 8,1 | The Webmin HTTP server (miniserv.pl) | Authentication Bypass by Spoofing | | https://github.com/webmin/webmin/releases/tag/2.641 Cybersecurity and Infrastructure Security Agency (CISA) U.S. Civilian Government https://raw.githubusercontent.com/cisagov/CSAF/develop/csaf_files/IT/white/2026/va-26-169-02.json Cybersecurity and Infrastructure Security Agency (CISA) U.S. Civilian Government https://webmin.com/security/#webmin-prior-to-2641 Cybersecu- |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | rity and Infrastructure Security Agency (CISA) U.S. Civilian Government https://www.cve.org/CVERecord?id=CVE-2026-56020 |
| https://nvd.nist.gov/vuln/detail/CVE-2026-43994 | 8,1 | Coturn | Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | prior to 4.10.0 | https://github.com/coturn/coturn/releases/tag/4.10.0 GitHub, Inc. https://github.com/coturn/coturn/security/advisories/GHSA-74pg-rfh2-5qw5 |
| https://nvd.nist.gov/vuln/detail/CVE-2026-12191 | 7,8 | Comma AI Openpilot | Improper Input Validation | 0.11 | https://vuldb.com/cve/CVE-2026-12191 |
| https://nvd.nist.gov/vuln/detail/CVE-2026-12193 | 7,8 | VS Revo RevoUninstaller | Improper Restriction of Operations within the Bounds of a Memory Buffer | 2.5.x/2.6.x | https://github.com/Kalagious/RevoDetectorExploit/tree/master |
| https://nvd.nist.gov/vuln/detail/CVE-2026-25865 | 7,8 | Punto Switcher | Unquoted Search Path or Element | through 4.5.0.583 | https://spektion.com/articles/cve-2026-25865-punto-switcher VulnCheck https://www.vulncheck.com/advisories/punto-switcher-unquoted-search-path-via-winexec VulnCheck https://yandex.ru/soft/punto |
| https://nvd.nist.gov/vuln/detail/CVE-2026-54017 | 7,7 | Open WebUI | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | Prior to 0.9.6 | https://github.com/open-webui/open-webui/security/advisories/GHSA-r2wg-2mcr-66rv |
| https://nvd.nist.gov/vuln/detail/CVE-2026-32174 | 7,7 | Azure Bot Service | Improper Authentication | | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32174 |
| https://nvd.nist.gov/vuln/detail/CVE-2026-6428 | 7,6 | reports/catalogue_out.pl in Koha Community | Improper Neutralization of Special Elements used in an | through 22.11.37, 23.x, 24.x before 24.11.16, 25.05.x before 25.05.11, | https://bugs.koha-community.org/bugzilla3/attachment.cgi?id=199539 |

| | | | | | |
|---|---|---|---|---|---|
| | | | SQL Command ('SQL Injection') | 25.11.x before 25.11.05, 26.05.x before 26.05.01, and 26.11.x before 26.11.00 | |
| https://nvd.nist.gov/vuln/detail/CVE-2026-55204 | 7,5 | HAProxy | NULL Pointer Dereference | through 3.4.0 | https://github.com/haproxy/haproxy/commit/9a6d1fe3f00d86ab4ea6ea6ea0a5d48fc058a513 VulnCheck https://www.vulncheck.com/advisories/haproxy-null-pointer-dereference-in-hpack-dht-insert-function |
| https://nvd.nist.gov/vuln/detail/CVE-2026-12200 | 7,3 | Ritlabs TinyWeb Server | Stack-based Buffer Overflow | up to 1.94 on Win32 | https://nathan2.com/posts/tinyweb/ VulDB https://vuldb.com/cve/CVE-2026-12200 VulDB https://vuldb.com/submit/829894 VulDB https://vuldb.com/vuln/370842 VulDB https://vuldb.com/vuln/370842/cti |
| https://nvd.nist.gov/vuln/detail/CVE-2026-9109 | 7,2 | The GPTranslate – Multilingual AI Translation for WordPress | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | up to, and including, 2.31 | https://plugins.trac.wordpress.org/browser/gptranslate/tags/2.27.5/assets/js/admin.js#L1 |
| https://nvd.nist.gov/vuln/detail/CVE-2026-5513 | 7,2 | The Online Scheduling and Appointment Booking System – Bookly plugin for WordPress | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | up to, and including, 27.2 | https://plugins.trac.wordpress.org/changeset/3504922/bookly-responsive-appointment-booking-tool Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/b8ab6dfa-3764-470f-aa49-1964f42d93de?source=cve |

## 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 Adds One Known Exploited Vulnerability to Catalog** | ▪ **CVE-2026-20253 Splunk Enterprise Missing Authentication for Critical Function Vulnerability** | **https://www.cisa.gov/news-events/alerts/2026/06/18/cisa-adds-one-known-exploited-vulnerability-catalog** |
| **CISA Urges Hardening Fortinet Devices After Reports of Credential Exposure** | | **https://www.cisa.gov/news-events/alerts/2026/06/18/cisa-urges-hardening-fortinet-devices-after-reports-credential-exposure** |

## 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 |
|---|---|
| **Fake GitHub Stars and AI Videos Mask a Crypto Clipper** | https://www.infosecurity-magazine.com/news/crypto-clipboard-hijacker-fake/ |
| **Hostile States Behind 75% of Cyber-Attacks on UK Critical Infrastructure, NCSC Warns** | https://www.infosecurity-magazine.com/news/hostile-states-cni-75-percent-ncsc/ |
| **North Korean Hiring Fraud Runs on AI and US Laptop Farms** | https://www.infosecurity-magazine.com/news/north-korea-it-worker-fraud-ai/ |
| **Serverless Phishing Kit on GitHub Targets Mexican Banks** | https://www.infosecurity-magazine.com/news/gitbait-github-pages-sheetbest/ |
| **Sensitive Enterprise Data Uploads to AI Models Double in a Year** | https://www.infosecurity-magazine.com/news/sensitive-ai-data-upload-doubles/ |
| AI-Powered Public Surveillance and Biometric Data Collection Expand Government Monitoring | https://cybersecuritynews.com/ai-powered-public-surveillance/ |
| **Authorities Dismantle SocGholish Malware Network — 106 Servers and 101 Domains Seized** | https://cybersecuritynews.com/authorities-dismantle-socgholish/ |
| **Microsoft Office Applications Might Fail to Open Following Windows 11 June Update** | https://cybersecuritynews.com/office-app-issues-windows-11-june-update/ |

## 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 |
|---|---|
| **Novo Nordisk Breach Exposes Software Development Pipeline Risk** | https://www.darkreading.com/cyber-risk/novo-nordisk-breach-exposes-dev-pipeline-risk |
| **Fifteen JetBrains Marketplace Plugins Found Stealing API Keys** | https://www.infosecurity-magazine.com/news/fifteen-jetbrains-marketplace/ |
| **Hackers Abuse Microsoft Fondue.exe to Side-Load APPWIZ.cpl and Execute Malware** | https://cybersecuritynews.com/hackers-abuse-microsoft-fondue-exe/ |
| Hackers Actively Exploiting WordPress SMTP Plugin With 100,000+ Installs to Access Sensitive Data | https://cybersecuritynews.com/hackers-exploiting-wordpress-smtp-plugin/ |

## 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 |
|---|---|
| **Critical Chrome Vulnerabilities Allow Attackers to Execute Arbitrary Code – Update Now!** | https://cybersecuritynews.com/chrome-vulnerabilities-execute-arbitrary-code/ |
| **Critical LiteLLM Flaw Allows Authentication Bypass via Host Header Injection** | https://cybersecuritynews.com/litellm-vulnerability-host-header-injection/ |
| CISA Warns of Actively Exploited Joomla JCE Flaw Allowing PHP Code Execution | https://thehackernews.com/2026/06/cisa-warns-of-actively-exploited-joomla.html |
| **Splunk Enterprise Vulnerability Exploited in Attacks Days After Disclosure** | https://www.securityweek.com/splunk-enterprise-vulnerability-exploited-in-attacks-days-after-disclosure/ |
| **New iPhone BootROM Vulnerability Exposes Apple SoCs to Full Chain-of-Trust Compromise** | https://cybersecuritynews.com/iphone-bootrom-vulnerability/ |
| **Hackers Breached Klue Integration to Steal Salesforce CRM Data via OAuth Tokens** | HTTPS://CYBERSECURITYNEWS.COM/KLUE-INTEGRATION-BREACHED-SALESFORCE/ |
| **Multiple Vulnerabilities in Firefox 152 Enables Remote Code Execution Attacks** | https://cybersecuritynews.com/firefox-152-vulnerabilities/ |
| **Critical Cisco ISE Vulnerability Allows Attacker to Execute Malicious Code Remotely** | https://cybersecuritynews.com/cisco-ise-rec-vulnerability/ |
| **PoC Exploit Released for HTTP/2 Bomb Remote DoS Vulnerability in Apache HTTP Server** | https://cybersecuritynews.com/http-2-bomb-dos-apache/ |

## 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 |
|---|---|
| **3 Recently Patched Fortinet FortiSandbox Vulnerabilities in Hacker Crosshairs** | https://www.securityweek.com/3-recently-patched-fortinet-fortisandbox-vulnerabilities-in-hacker-crosshairs/ |
| Apple Patches Beats Studio Buds Flaw Letting Nearby Attackers Spy via Microphone | https://thehackernews.com/2026/06/apple-patches-beats-studio-buds-flaw.html |
| F5 Patches Two Critical NGINX Open Source Flaws Enabling Remote Code Execution | https://thehackernews.com/2026/06/f5-patches-two-critical-nginx-open.html |
| **Atlassian, Splunk Patch Critical Vulnerabilities** | https://www.securityweek.com/atlassian-splunk-patch-critical-vulnerabilities/ |
| **Critical Command Execution Vulnerability Patched in Cisco ISE** | https://www.securityweek.com/critical-command-execution-vulnerability-patched-in-cisco-ise/ |
| **Rockwell Automation Patches Vulnerabilities in ICS Controllers and Software** | https://www.securityweek.com/rockwell-automation-patches-vulnerabilities-in-ics-controllers-and-software/ |
| **Microsoft Working on Patch for 'RoguePlanet' Zero-Day** | https://www.securityweek.com/microsoft-working-on-patch-for-rogueplanet-zero-day/ |
| **Oracle's Second Monthly Security Updates Deliver 245 Patches** | https://www.securityweek.com/oracles-second-monthly-security-updates-deliver-245-patches/ |
| **Chrome and Firefox Updated to Patch Critical, High-Severity Vulnerabilities** | https://www.securityweek.com/chrome-and-firefox-updated-to-patch-critical-high-severity-vulnerabilities/ |

## 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 |
|---|---|
| **Ghostwriter Hackers Abuse Gmail Admin-Themed Emails to Steal Credentials and 2FA Codes** | https://cybersecuritynews.com/ghostwriter-hackers-abuse-gmail-admin-themed-emails/ |
| **ClickFix Campaign Uses EtherHiding and GULoader to Infect Windows Users via Fake CAPTCHA** | https://cybersecuritynews.com/clickfix-campaign-uses-etherhiding-and-guloader/ |
| **New OnionDrop Loader Campaign Uses gainmsg C2 to Deliver LegionLoader Payloads** | https://cybersecuritynews.com/new-oniondrop-loader-campaign-uses-gainmsg-c2/ |
| **UNC3753 Uses Screen-Sharing Sessions and RMM Tools to Exfiltrate Sensitive Legal Data** | https://cybersecuritynews.com/unc3753-uses-screen-sharing-sessions-and-rmm-tools/ |
| **Hackers Using Claude and OpenAI's Codex for Exploitation, and Data Exfiltration Activities** | https://cybersecuritynews.com/hackers-using-claude-and-openais-codex-exploitation/ |
| **Deno-Based RAT Uses Microsoft Teams Impersonation and Mailbombing to Target Employees** | https://cybersecuritynews.com/hackers-use-rokarolla-android-malware/ |
| **Hackers Use Rokarolla Android Malware to Disable Google Play Protect and Control Devices** | https://cybersecuritynews.com/hackers-use-rokarolla-android-malware-2/ |
| INC Ransomware Emerges as Major RaaS Threat in 2026 with 830+ Victims Since 2023 | https://thehackernews.com/2026/06/inc-ransomware-claims-830-victims-since.html |

| | |
|---|---|
| **Hackers Can Leverage SQL Server 2025 AI Features to Exfiltrate Sensitive Data** | https://cybersecuritynews.com/hackers-leverage-sql-server-2025-ai-features/ |
| **Hackers Abuse Claude.ai Shared Chat Feature to Host the ClickFix Social Engineering Instructions** | https://cybersecuritynews.com/claude-ai-shared-chat-feature-abused/ |
| **Hackers Abuse PowerShell Commands to Deliver SmartRAT Through Brazilian Bank Phishing Page** | https://cybersecuritynews.com/hackers-abuse-powershell-commands/ |

## 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/** |
| Splunk Releases Guide to Detect Remote Employment Fraud Within Your Organization | https://cybersecuritynews.com/detect-remote-employment-fraud/ |
| 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/ |
| **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/ |
| **GitLab Security Best Practices Cheat Sheet** | https://thehackernews.uk/gitlab-security-tips |
| False Negatives Are a New SOC Headache. Here's the Fast Way to Fix It | https://cybersecuritynews.com/false-negatives-are-a-new-soc-headache-heres-the-fast-way-to-fix-it/ |
| PentAGI – Automated AI-Powered Penetration Testing Tool that Integrates 20+ Security Tools | https://cybersecuritynews.com/pentagi-penetration-testing-tool/ |
| **The CISO Executive Toolkit (Free Download)** | https://thehackernews.uk/wiz-ciso-bundle |
| **Secure Coding Best Practices: Practical Guide + Cheat Sheet for Developers** | https://thehackernews.uk/secure-coding-wiz-cheat |
| **Top 10 Best Malware Sandbox Tools for Security Teams in 2026** | https://cybersecuritynews.com/best-malware-sandbox-tools/ |
| **Top 5 Best Tools for Simulated DDoS Attacks in 2026** | https://cybersecuritynews.com/simulated-ddos-attacks/ |

# 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/ |