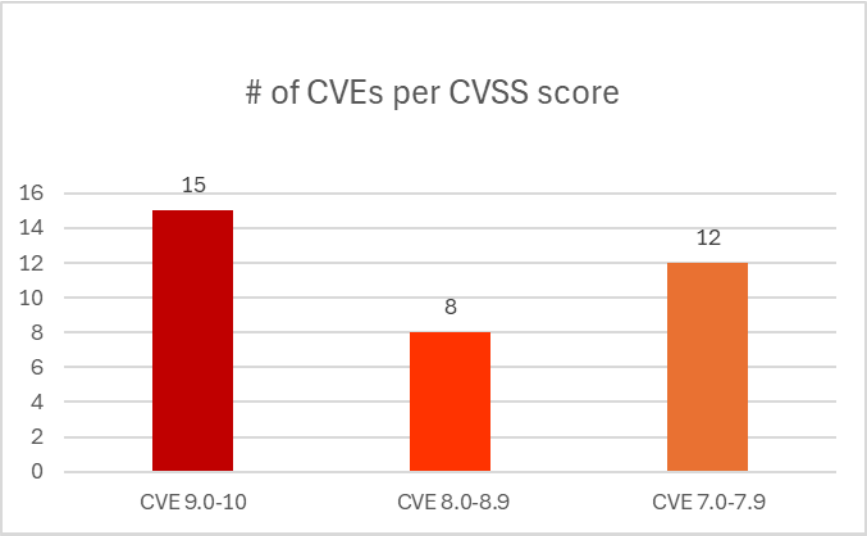
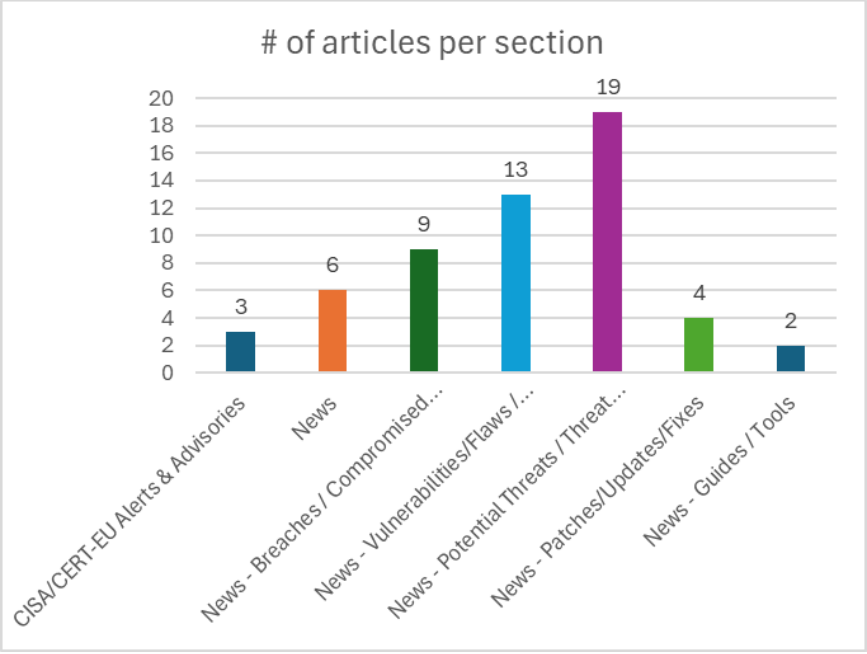
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 27/05/2026 - 29/05/2026





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)	CVS Sv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2026-43898	10,0	SandboxJS	Improper Control of Generation of Code ('Code Injection')	Prior to 0.9.6	https://github.com/nyariv/SandboxJS/commit/826865251232611ec94078bab5a18ec875dad4a5 GitHub, Inc. https://github.com/nyariv/SandboxJS/security/advisories/GHSA-g8f2-4f4f-5jqw
https://nvd.nist.gov/vuln/detail/CVE-2026-44330	10,0	free5GC	Incorrect Authorization	free5GC is an open-source implementation of the 5G core network. Prior to 4.2.2	https://github.com/free5gc/free5gc/security/advisories/GHSA-rwww-x45w-p52w
https://nvd.nist.gov/vuln/detail/CVE-2026-46840	10,0	Oracle	-	Oracle REST Data Services 24.2.0-26.1.0	https://www.oracle.com/security-alerts/cspumay2026.html
https://nvd.nist.gov/vuln/detail/CVE-2026-8054	10,0	dotCMS Core	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	dotCMS Core 25.11.04-1 through 26.04.28-02	https://dev.dotcms.com/docs/known-security-issues?issueNumber=SI-75 https://github.com/dotCMS/core/pull/35553
https://nvd.nist.gov/vuln/detail/CVE-2026-7374	9,9	Red Hat, Inc.	Improper Link Resolution Before File Access ('Link Following')	-	https://access.redhat.com/errata/RHSA-2026:20720 https://access.redhat.com/errata/RHSA-2026:20736 https://access.redhat.com/errata/RHSA-2026:20763 https://access.redhat.com/errata/RHSA-2026:20767 https://access.redhat.com/errata/RHSA-2026:20782 https://access.redhat.com/errata/RHSA-2026:20825 https://access.redhat.com/errata/RHSA-2026:20866 https://access.redhat.com/errata/RHSA-2026:20886 https://access.redhat.com/errata/RHSA-2026:20890 https://access.redhat.com/errata/RHSA-2026:20975 https://access.redhat.com/security/cve/CVE-2026-7374 https://bugzilla.redhat.com/show_bug.cgi?id=2463728
https://nvd.nist.gov/vuln/detail/CVE-2026-9645	9,9	Tenable Network Security, Inc.	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	-	https://www.tenable.com/security/research/tra-2026-46
https://nvd.nist.gov/vuln/detail/CVE-2026-24212	9,8	NVIDIA	Cleartext Transmission of Sensitive Information	NVIDIA Isaac Launchable for Linux	https://nvd.nist.gov/vuln/detail/CVE-2026-24212 https://nvidia.custhelp.com/app/answers/detail/a_id/5830 https://www.cve.org/CVERecord?id=CVE-2026-24212

https://nvd.nist.gov/vuln/detail/CVE-2026-3660	9,8	IBM Engineering Lifecycle Management	Incorrect Authorization	IBM Engineering Lifecycle Management 7.0.3, 7.1.0, and 7.2.0	https://www.ibm.com/support/pages/node/7274079
https://nvd.nist.gov/vuln/detail/CVE-2026-38707	9,8	InHand Networks	Improper Neutralization of Special Elements used in a Command ('Command Injection')	IPSec VPN feature of InHand Networks IR302 firmware V3.5.108, IR305 firmware V1.0.118, IR315 firmware V1.0.118, IR615 firmware V1.0.118, and earlier versions	https://www.inhand.com/wp-content/uploads/InHand-PSA-2026-05_EN.pdf
https://nvd.nist.gov/vuln/detail/CVE-2026-48027	9,8	Nx & Lerna	Embedded Malicious Code	Nx Console, 18.95.0	https://github.com/nrwl/nx-console/issues/3139 https://github.com/nrwl/nx-console/security/advisories/GHSA-c9j4-9m59-847w https://nx.dev/blog/nx-console-v18-95-0-postmortem#indicators-of-compromise https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-48027 https://www.stepsecurity.io/blog/nx-console-vs-code-extension-compromised
https://nvd.nist.gov/vuln/detail/CVE-2026-48172	9,8	LiteSpeed	Incorrect Privilege Assignment	LiteSpeed User-End cPanel Plugin before 2.4.5	https://blog.litespeedtech.com/2026/05/21/security-update-for-litespeed-cpanel-plugin/ https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-48172 https://www.litespeedtech.com/products/litespeed-web-server/control-panel-support/cpanel https://www.litespeedtech.com/products/litespeed-web-server/control-panel-support/release-log
https://nvd.nist.gov/vuln/detail/CVE-2026-48904	9,8	Joomla! Project	Insufficient Information	-	https://developer.joomla.org/security-centre/1046-20260514-core-privilege-escalation-through-com-users-webservice-endpoints.html
https://nvd.nist.gov/vuln/detail/CVE-2026-8398	9,8	DAEMON Tools Lite	Embedded Malicious Code	DAEMON Tools Lite (Windows versions 12.5.0.2421 through 12.5.0.2434)	https://blog.daemon-tools.cc/post/security-incident https://securelist.com/tr/daemon-tools-backdoor/119654/ https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-8398
https://nvd.nist.gov/vuln/detail/CVE-2026-9170	9,8	IBM HTTP Server	Improper Control of Generation of Code ('Code Injection')	IBM HTTP Server 8.5, and 9.0	https://www.ibm.com/support/pages/node/7274065
https://nvd.nist.gov/vuln/detail/CVE-2026-9543	9,8	Totolink	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Totolink N300RH 6.1c.1353_B20190305	https://github.com/A1ester/TOTOLINK-N300RH-Command-Injection https://vuldb.com/submit/815068 https://vuldb.com/vuln/365607 https://vuldb.com/vuln/365607/cti https://www.totolink.net/
https://nvd.nist.gov/vuln/detail/CVE-2026-46414	8,8	Microsoft	Authentication Bypass by Spoofing	Microsoft UFO open-source framework for intelligent automation across devices and platforms. In 3.0.1-4-ge2626659	https://github.com/microsoft/UFO/security/advisories/GHSA-qgx6-cvhg-jw7p

https://nvd.nist.gov/vuln/detail/CVE-2026-46837	8,8	Oracle	-	Oracle Flow Manufacturing product of Oracle E-Business Suite (component: Security)	https://www.oracle.com/security-alerts/cspumay2026.html
https://nvd.nist.gov/vuln/detail/CVE-2026-8915	8,8	Samsung	Out-of-bounds Write	Samsung Open Source Escargot	https://github.com/Samsung/escargot/pull/1579
https://nvd.nist.gov/vuln/detail/CVE-2025-30028	8,6	Synology Inc.	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Active Backup for Business	https://www.synology.com/en-global/security/advisory/Synology_SA_25_02
https://nvd.nist.gov/vuln/detail/CVE-2026-7365	8,4	IBM	Use of Default Credentials	IBM Operations Analytics - Log Analysis and IBM SmartCloud Analytics - Log Analysis	https://www.ibm.com/support/pages/node/7272268
https://nvd.nist.gov/vuln/detail/CVE-2026-35277	8,1	Oracle	-	Oracle REST Data Services (component: Core)	https://www.oracle.com/security-alerts/cspumay2026.html
https://nvd.nist.gov/vuln/detail/CVE-2026-46828	8,1	Oracle	-	Oracle E-Business Suite (component: Internal Operations)	https://www.oracle.com/security-alerts/cspumay2026.html
https://nvd.nist.gov/vuln/detail/CVE-2026-6957	8,0	Mattermost, Inc.	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Mattermost Plugins versions <=1.1.5	https://mattermost.com/security-updates
https://nvd.nist.gov/vuln/detail/CVE-2026-47333	7,8	Ubuntu Linux	Out-of-bounds Read	Ubuntu Linux 6.8, 6.17 and 7.0	https://git.launchpad.net/~ubuntu-kernel/ubuntu/+source/linux/+git/noble/commit/?id=635fa30ed9e944bdb7e811fb8a8906286b4b4f06
https://nvd.nist.gov/vuln/detail/CVE-2026-49237	7,8	Canonical Multipass	Incorrect Default Permissions	Canonical Multipass for macOS before version 1.16.3	https://github.com/canonical/multipass/security/advisories/GHSA-r2xg-x32f-23c5
https://nvd.nist.gov/vuln/detail/CVE-2026-2253	7,7	Hitachi	Improper Restriction of XML External Entity Reference	Hitachi Vantara Pentaho Data Integration & Analytics versions before 10.2.0.7 and 11.0.0.0, including 9.3.x and 8.3.x	https://support.pentaho.com/hc/en-us/articles/45677548193933--Resolved-Hitachi-Vantara-Pentaho-Data-Integration-Analytics-Improper-Restriction-of-XML-External-Entity-Reference-Versions-before-10-2-0-7-and-11-0-0-0-Impacted-CVE-2026-2253
https://nvd.nist.gov/vuln/detail/CVE-2026-46821	7,7	Oracle	-	Oracle Financials Common Modules product of Oracle E-Business Suite (component: Common Components)	https://www.oracle.com/security-alerts/cspumay2026.html
https://nvd.nist.gov/vuln/detail/CVE-2026-46829	7,5	Oracle	-	Oracle REST Data Services (component: Mongoapi)	https://www.oracle.com/security-alerts/cspumay2026.html

https://nvd.nist.gov/vuln/detail/CVE-2026-46835	7,5	Oracle	-	Oracle Database Server	https://www.oracle.com/security-alerts/cspumay2026.html
https://nvd.nist.gov/vuln/detail/CVE-2026-48922	7,5	Jenkins Project	Improper Input Validation	Jenkins Credentials Binding Plugin 720.v3f6decef43ea_ and earlier	https://www.jenkins.io/security/advisory/2026-05-27/#SECURITY-3790
https://nvd.nist.gov/vuln/detail/CVE-2026-6052	7,5	IBM	Uncontrolled Resource Consumption	IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.4	https://www.ibm.com/support/pages/node/7273557
https://nvd.nist.gov/vuln/detail/CVE-2026-6938	7,5	IBM	Improper Authorization	IBM Db2 12.1.0 through 12.1.4	https://www.ibm.com/support/pages/node/7273559
https://nvd.nist.gov/vuln/detail/CVE-2026-8180	7,5	IBM	NULL Pointer Dereference	IBM Aspera High-Speed Transfer End-point 3.7.4 through 4.4.7 Fix Pack 1 and IBM Aspera High-Speed Transfer Server 3.7.4 through 4.4.7 Fix Pack 1 and IBM Aspera High-Speed Transfer Endpoint	https://www.ibm.com/support/pages/node/7273615
https://nvd.nist.gov/vuln/detail/CVE-2024-56462	7,2	IBM	Exposure of Backup File to an Unauthor-ized Control Sphere	IBM QRadar 7.5.0 through 7.5.0 UP15 In-terim Fix 002	https://www.ibm.com/support/pages/node/7273957
https://nvd.nist.gov/vuln/detail/CVE-2026-49000	7,0	ZTE Corporation	Cryptographic Issues	-	https://support.zte.com.cn/zte-iccp-isupport-webui/bulletin/detail/3711746568357343394

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-2026-48172 LiteSpeed cPanel Plugin Privilege Escalation Vulnerability	https://www.cisa.gov/news-events/alerts/2026/05/26/cisa-adds-one-known-exploited-vulnerability-catalog
CISA Adds Three Known Exploited Vulnerabilities to Catalog	▪ CVE-2026-8398 Daemon Tools Lite Embedded Malicious Code Vulnerability ▪ CVE-2026-45321 TanStack Unspecified Vulnerability ▪ CVE-2026-48027 Nx Console Embedded Malicious Code Vulnerability	https://www.cisa.gov/news-events/alerts/2026/05/27/cisa-adds-three-known-exploited-vulnerabilities-catalog
Supply Chain Compromises Impact Nx Console and GitHub Repositories		https://www.cisa.gov/news-events/alerts/2026/05/28/supply-chain-compromises-impact-nx-console-and-github-repositories

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
Google Employee Charged for Making $1.2 Million With Confidential Information	https://cybersecuritynews.com/google-employee-charged-for-making-1-2-million-with-confidential-information/
AI-Generated npm Malware Accidentally Exposes Threat Actor’s Private GitHub Token	https://cybersecuritynews.com/ai-generated-npm-malware/
Claude Opus 4.8 Released With Ability to Work as an Experienced Engineer	https://cybersecuritynews.com/claude-opus-4-8-released/
How Top CISOs Increase Risk Visibility for Zero Critical Incidents	https://cybersecuritynews.com/how-top-cisos-increase-risk-visibility-for-zero-critical-incidents/
Apple’s New Anti-Snatching Feature Will Auto-Lock iPhones When Stolen From Your Hand	https://cybersecuritynews.com/apple-anti-snatching-auto-lock-iphones/
GitLab Suspends Windows Exploit Researcher Nightmare-Eclipse After GitHub Ban	https://cybersecuritynews.com/windows-exploit-researcher-suspended/

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
Hackers Exploit Microsoft Teams' Collaboration Features to Impersonate IT Helpdesk Staff	https://cybersecuritynews.com/microsoft-teams-collaboration-features-exploited/
Carnival Cruise Data Breach Exposes Millions of Customers' Personal Information	https://cybersecuritynews.com/carnival-cruise-data-breach/
Hackers Abuse Shared CDN Edge IPs to Bypass Protective DNS Filtering	https://cybersecuritynews.com/cdn-edge-ips-bypass-dns-filtering/
Threat Actors Spoofing FIFA Websites to Steal Name, Home Address, and Phone Number	https://cybersecuritynews.com/spoofing-fifa-websites-to-steal/
Motorola Phones Preinstalled App Found Hijacking Amazon App to Inject Affiliate Codes	https://cybersecuritynews.com/motorola-phones-hijacking-amazon-app/
Seedworm APT Abuses Signed Fortemedia and SentinelOne Binaries for DLL Side-loading	https://cybersecuritynews.com/seedworm-apt-abuses-signed-fortemedia-2/
Hackers Abuse Trusted Google Domains to Hide Phishing Links From Email Gateways	https://cybersecuritynews.com/hackers-abuse-trusted-google-domains/
Developer-Targeting Glassworm Malware Abuses npm, PyPI, OpenVSX, and GitHub	https://cybersecuritynews.com/developer-targeting-glassworm-malware-abuses-npm/
Attackers Abuse Open RDP Ports to Gain Initial Access Into Business Networks	https://cybersecuritynews.com/attackers-abuse-open-rdp-ports/

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
New Gogs 0-Day Vulnerability Lets Attackers Run Malicious Code on the Server Remotely	https://cybersecuritynews.com/gogs-0-day-vulnerability/
Critical OpenVPN Connect for macOS Vulnerability Let Attackers Execute Arbitrary Commands	https://cybersecuritynews.com/openvpn-connect-for-macos-vulnerability/
New Linux CIFSwitch Kernel Vulnerability Allows Attackers to Gain Root Access	https://cybersecuritynews.com/linux-cifswitch-kernel-vulnerability/
Gitea Container Vulnerability Exposes Private Container Images to Attackers	https://cybersecuritynews.com/gitea-container-vulnerability/
Critical Roundcube Webmail Vulnerability Let Attackers Inject SQL Queries	https://cybersecuritynews.com/roundcube-webmail-sql-vulnerability/
Veeam Backup & Replication Tool Vulnerability Enables Privilege Escalation Attacks	https://cybersecuritynews.com/veeam-backup-replication-tool-vulnerability/
Microsoft Warns Public Release of Zero-Day Details Before Vendor Coordination	https://cybersecuritynews.com/microsoft-public-release-zero-day/
Critical Notepad++ Vulnerabilities Allow Attackers to Execute Arbitrary Code	https://cybersecuritynews.com/critical-notepad-vulnerabilities/
FortiClient EMS Code Execution Vulnerability Exploited to Deploy EKZ Malware	https://cybersecuritynews.com/forticlient-code-execution-vulnerability/
Critical Fortinet FortiClient EMS 0-Day Vulnerability Actively Exploited in the Wild	https://cybersecuritynews.com/fortinet-forticlient-ems-0-day/
CISA Warns of LiteSpeed cPanel Plugin Vulnerability Exploited in Attacks	https://cybersecuritynews.com/litespeed-cpanel-plugin-vulnerability-exploit/
Windows Kernel Vulnerability Allows Attackers to Modify Kernel Memory Counters	https://cybersecuritynews.com/windows-kernel-vulnerability/
BIND 9 Software Vulnerabilities Exposes Resolvers and Authoritative Servers to Remote Exploits	https://cybersecuritynews.com/bind-9-vulnerabilities-exposes/

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
Google Patches 151 Vulnerabilities in Chrome, Including 22 Critical Ones	https://cybersecuritynews.com/151-chrome-vulnerabilities-patched/
Anthropic Updates Claude Code With Security Plugin and Faster Performance	https://cybersecuritynews.com/anthropic-updates-claude-code/
GitHub Enterprise Server 3.20.3 Released With Fox for Critical Vulnerabilities	https://cybersecuritynews.com/github-enterprise-server-3-20-3/
Anthropic Releases Free Security Plugin for Claude Code Terminal to Detect Vulnerabilities	https://cybersecuritynews.com/free-security-plugin-for-claude-code/

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
Malicious RVTools Installer Abuses Sectigo Certificate to Bypass SmartScreen Warn-ings	https://cybersecuritynews.com/malicious-rvtools-installer-abuses-sectigo-certificate/
Critical Samba Vulnerability Enables Remote Code Execution Attacks	https://cybersecuritynews.com/samba-rce-vulnerability/
VS Code Remote-SSH RCE Lets Attackers Pivot From Developer Machines to Cloud Servers	https://cybersecuritynews.com/vs-code-remote-ssh-rce/
Hackers Use LLM Agent to Move From Marimo RCE to Internal Database in Four Piv-ots	https://cybersecuritynews.com/hackers-use-llm-agent-to-move-from-marimo-rce/
VaultJacking Attack Steals Entire Google Password Manager Vault With One Cap-tured PIN	https://cybersecuritynews.com/vaultjacking-attack-steals-entire-google-password-manager/
Hackers Deploy VIP Keylogger Through Phishing Emails Masquerading as Business Documents	https://cybersecuritynews.com/hackers-deploy-vip-keylogger-through-phishing-emails/
ClearFake Uses BSC Testnet Smart Contracts for Takedown-Resistant Command and Control	https://cybersecuritynews.com/clearfake-uses-bsc-testnet-smart-contracts/
Malicious Websites Track Visitors by Analyzing their SSD Timing Activity	https://cybersecuritynews.com/malicious-websites-track-ssd-timing/
Hackers Use GHOSTYNETWORKS and OMEGATECH to Host JS Malware Infrastruc-ture	https://cybersecuritynews.com/hackers-use-ghostynetworks-and-omegatech/
New PureLogs Variant Uses MsBuild.exe Process Hollowing to Evade Detection	https://cybersecuritynews.com/new-purelogs-variant-uses-msbuild-exe-process-hollowing/
Silent Ransom Group Targets Law Firms With IT Support Impersonation Attacks	https://cybersecuritynews.com/silent-ransom-group-targets-law-firms/
GHOST STADIUM Phishing Campaign Targets FIFA World Cup Fans With 300+ Fake Domains	https://cybersecuritynews.com/ghost-stadium-phishing-campaign-targets-fifa-world-cup-fans/
Tycoon 2FA AiTM Kit Bypasses MFA on Entra ID and Google Workspace Accounts	https://cybersecuritynews.com/tycoon-2fa-aitm-kit-bypasses-mfa/
Hackers Use Fake ChatGPT and Claude Installers to Deploy DinDoor Backdoor	https://cybersecuritynews.com/hackers-use-fake-chatgpt-and-claude-installers/
Hackers Push 22 Versions of npm RAT With Wallet Theft and Persistent Backdoor	https://cybersecuritynews.com/hackers-push-22-versions-of-npm-rat/
Hackers Abuse AI Chatbot Recommendations to Push Malicious Software Download Links	https://cybersecuritynews.com/hackers-abuse-ai-chatbot-recommendations/
Attackers Can Exploit BadHost to Access Sensitive AI Agent Server Endpoints	https://cybersecuritynews.com/badhost-ai-agent-vulnerability/
New BTMOB Malware Lets Attackers Remotely Control Android Devices	https://cybersecuritynews.com/btmob-malware-control-android-devices/
New 0-Click WhatsApp Account Takeover Attack Targeting iOS 16 Users	https://cybersecuritynews.com/0-click-whatsapp-target-ios-16-users/

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 10 Best Mobile Application Security Testing (MAST) Tools in 2026	https://cybersecuritynews.com/best-mast-tools/
Top 10 Best Static Application Security Testing (SAST) Tools for Security Teams in 2026	https://cybersecuritynews.com/best-sast-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/ 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 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 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/