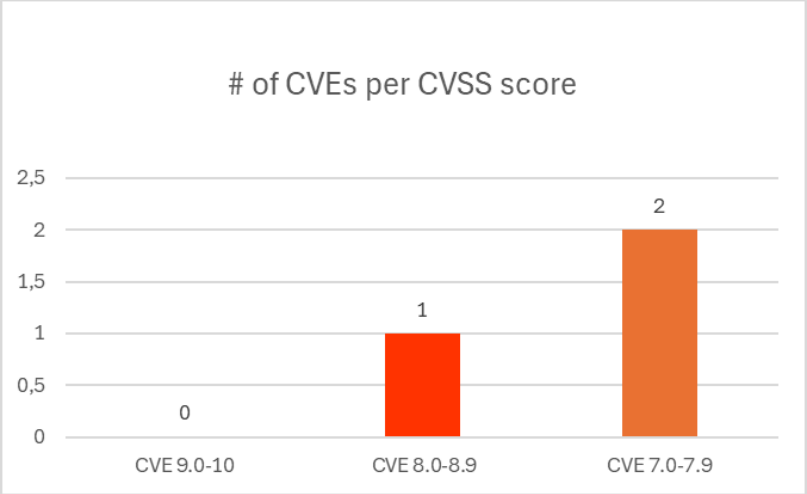
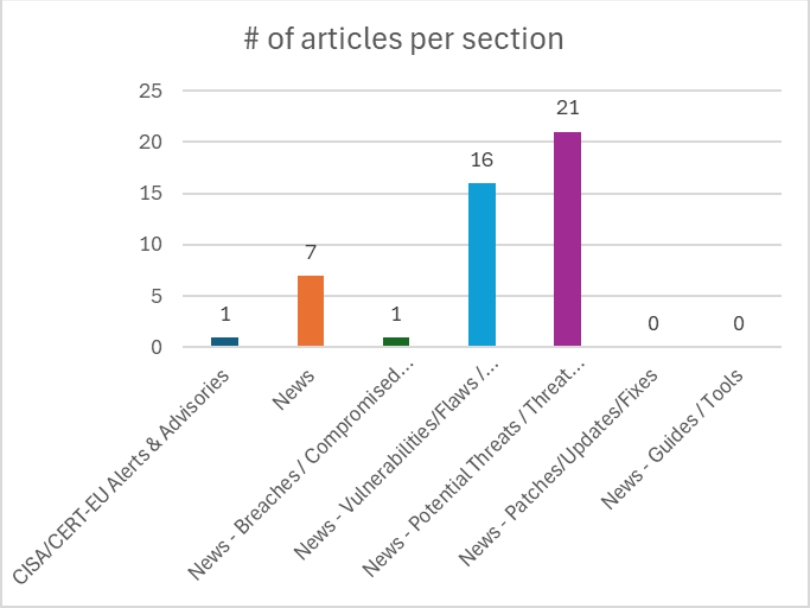
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 04/02/2026 - 06/02/2026





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)	CVSS v3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2025-23236	8,8	Defense Platform	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	Defense Platform Home Edition Ver.3.9.51.x and earlier	https://jvn.jp/en/jp/JVN66673020/ https://www.humming-heads.co.jp/dep/storelist/
https://nvd.nist.gov/vuln/detail/CVE-2018-20834	7,5	node-tar	Improper Link Resolution Before File Access ('Link Following')	node-tar before version 4.4.2 (excluding version 2.2.2)	https://access.redhat.com/errata/RHSA-2019:1821 https://github.com/npm/node-tar/commit/7ecef07da6a9e72cc0c4d0c9c6a8e85b6b52395d https://github.com/npm/node-tar/commit/b0c58433c22f5e7fe8b1c76373f27e3f81dcd4c8 https://github.com/npm/node-tar/commits/v2.2.2 https://github.com/npm/node-tar/compare/58a8d43...a5f7779 https://hackerone.com/reports/344595 CVE, MITRE https://nvd.nist.gov/vuln/detail/CVE-2018-20834
https://nvd.nist.gov/vuln/detail/CVE-2026-24714	7,5	NETGEAR	Inclusion of Undocumented Features or Chicken Bits		https://jvn.jp/en/jp/JVN46722282/ https://www.netgear.com/about/eos/

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 Two Known Exploited Vulnerabilities to Catalog	▪ CVE-2025-11953 React Native Community CLI OS Command Injection Vulnerability ▪ CVE-2026-24423 SmarterTools SmarterMail Missing Authentication for Critical Function Vulnerability	https://www.cisa.gov/news-events/alerts/2026/02/05/cisa-adds-two-known-exploited-vulnerabilities-catalog

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
New Epstein Tool Searches LinkedIn Connections Against 3.5 Million Pages Epstein Files	https://cybersecuritynews.com/epstein-tool/
Hackers Exploit SonicWall SSLVPN Credentials to Deploy EDR Killer and Bypass Security	https://cybersecuritynews.com/edr-killer-via-sonicwall-sslvpn/
Threat Actors Hacking NGINX Servers to Redirect Web Traffic to Malicious Servers	https://cybersecuritynews.com/threat-actors-hacking-nginx-servers/
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/
Hackers Using AI to Get AWS Admin Access Within 10 Minutes	https://cybersecuritynews.com/aws-admin-access-in-minutes/
Microsoft Investigating Teams Chat Image Retrieval Issue Affecting Enterprise Users	https://cybersecuritynews.com/teams-chats-image-retrieval/
Microsoft to Add Sysmon Threat Detection Feature Natively to Windows 11	https://cybersecuritynews.com/microsoft-to-add-sysmon-threat-detection-feature-natively-to-windows-11/

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
Betterment Data Breach Exposes 1.4 million Customers Personal Details	https://cybersecuritynews.com/betterment-data-breach/

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
F5 Patches Critical Vulnerabilities in BIG-IP, NGINX, and Related Products	https://cybersecuritynews.com/f5-patches-critical-vulnerabilities/
CISA Warns of React Native Community Command Injection Vulnerability Exploited in Attacks	https://cybersecuritynews.com/react-native-command-injection-flaw/
New CentOS 9 Vulnerability Lets Attackers Escalate to Root Privileges – PoC Released	https://cybersecuritynews.com/centos-9-vulnerability/
170+ SolarWinds Help Desk Installations Vulnerable to RCE Attacks Exposed Online	https://cybersecuritynews.com/solarwinds-help-desk-installations-vulnerable/
WatchGuard VPN Client for Windows Vulnerability Enables Command Execution With SYSTEM Privileges	https://cybersecuritynews.com/watchguard-vpn-client-for-windows-vulnerability/
Critical n8n Vulnerability Enables System Command Execution Via Weaponized Workflows	https://cybersecuritynews.com/n8n-rce-vulnerability/
Cisco Meeting Management Vulnerability Let Remote Attacker Upload Arbitrary Files	https://cybersecuritynews.com/cisco-meeting-management-upload-vulnerability/
CISA Warns of VMware ESXi 0-day Vulnerability Exploited in Ransomware Attacks	https://cybersecuritynews.com/vmware-esxi-0-day-ransomware-attack/
Multiple TP-Link OS Command Injection Vulnerabilities Let Attackers Gain Admin Control of the Device	https://cybersecuritynews.com/tp-link-os-command-injection-vulnerability/
CISA Warns of GitLab Community and Enterprise Editions SSRF Vulnerability Exploited in Attacks	https://cybersecuritynews.com/cisa-warns-gitlab-ssrf-vulnerability-exploit/
Hackers Actively Scanning Citrix NetScaler Infrastructure to Discover Login Panels	https://cybersecuritynews.com/scanning-citrix-netscaler-login/
Ingress-Nginx Vulnerability Allow Attackers to Execute Arbitrary Code	https://cybersecuritynews.com/ingress-nginx-vulnerability/
CISA Warns of SolarWinds Web Help Desk RCE Vulnerability Exploited in Attacks	https://cybersecuritynews.com/solarwinds-web-help-desk-rce-vulnerability-2/
Critical Django Vulnerabilities Enables DoS and SQL Injection Attacks	https://cybersecuritynews.com/django-vulnerabilities/
Chrome Vulnerabilities Let Attackers Execute Arbitrary Code and Crash System	https://cybersecuritynews.com/chrome-vulnerabilities-arbitrary-code-2/

Hackers Exploiting React Server Components Vulnerability in the Wild to Deploy Malicious Payloads	https://cybersecuritynews.com/react-server-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

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
Hackers Leveraging Windows Screensaver to Deploy RMM Tools and Gain Remote Access to Systems	https://cybersecuritynews.com/hackers-leveraging-windows-screensaver/
Spam Campaign Distributes Fake PDFs, Installing Remote Monitoring Tools for Persistent Access	https://cybersecuritynews.com/spam-campaign-distributes-fake-pdfs/
Attackers Mimic RTO Challan Notifications to Deliver Android Malware	https://cybersecuritynews.com/attackers-mimic-rto-challan-notifications/
ShadowSyndicate Using Server Transition Technique in Ransomware Attacks	https://cybersecuritynews.com/shadowsyndicate-using-server-transition/
Beware of Fake Traffic Ticket Portals that Harvest Your PII and Credit Card Data	https://cybersecuritynews.com/beware-of-fake-traffic-ticket-portals/
DragonForce Ransomware Attacking Critical Business to Exfiltrate Sensitive Information	https://cybersecuritynews.com/dragonforce-ransomware-attacking-critical-business/
Beware of Weaponized Voicemail Messages Granting Hackers Remote Access to Your System	https://cybersecuritynews.com/beware-of-weaponized-voicemail-messages/
APT28 Hackers Exploiting Microsoft Office Vulnerability to Compromise Government Agencies	https://cybersecuritynews.com/apt28-hackers-exploiting-microsoft-office-vulnerability/
New DesckVB RAT with Multi-stage Infection Chain and Plugin-Based Architecture	https://cybersecuritynews.com/new-desckvb-rat-with-multi-stage-infection-chain/
New 3 Step Malvertising Chain Abusing Facebook Paid Ads to Push Tech Support Scam Kit	https://cybersecuritynews.com/new-3-step-malvertising-chain-abusing-facebook-paid-ads/
Attackers Using DNS TXT Records in ClickFix Script to Execute Powershell Commands	https://cybersecuritynews.com/attackers-using-dns-txt-records-in-clickfix-script/
Amaranth-Dragon Exploiting WinRAR Vulnerability to Gain Persistent to Victim Systems	https://cybersecuritynews.com/amaranth-dragon-exploiting-winrar-vulnerability/

SystemBC Botnet Hijacked 10,000 Devices Worldwide to Use for DDoS Attacks	https://cybersecuritynews.com/systembc-botnet-hijacked-10000-devices/
PhantomVAI Custom Loader Uses RunPE Utility to Attack Users	https://cybersecuritynews.com/phantomvai-custom-loader/
Interlock Ransomware Actors New Tool Exploiting Gaming Anti-Cheat Driver 0-Day to Disable EDR and AV	https://cybersecuritynews.com/interlock-ransomware-actors-new-tool-exploiting-gaming-anti-cheat-driver-0-day/
Supply Chain Attack Abused Notepad++ Update Infrastructure to Deliver Targeted Malware	https://cybersecuritynews.com/supply-chain-attack-abused-notepad-update-infrastructure/
ValleyRAT Mimic as LINE Installer Attacking Users to Steal Login Details	https://cybersecuritynews.com/valleyrat-mimic-as-line-installer-attacking-users/
Threat Actors Abuse Microsoft & Google Platforms to Attack Enterprise Users	https://cybersecuritynews.com/threat-actors-abuse-microsoft-google-platforms/
Shadow DNS Hacking Routers Internet Traffic Through Compromised Routers	https://cybersecuritynews.com/shadow-dns-hacking-routers-internet-traffic/
Hackers Exfiltrating NTDS.dit File to Gain Full Active Directory Access	https://cybersecuritynews.com/hackers-exfiltrating-ntds-dit-file/
GlassWorm Infiltrated VSX Extensions with More than 22,000 Downloads to Attack Developers	https://cybersecuritynews.com/glassworm-infiltrated-vsx-extensions/

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

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/