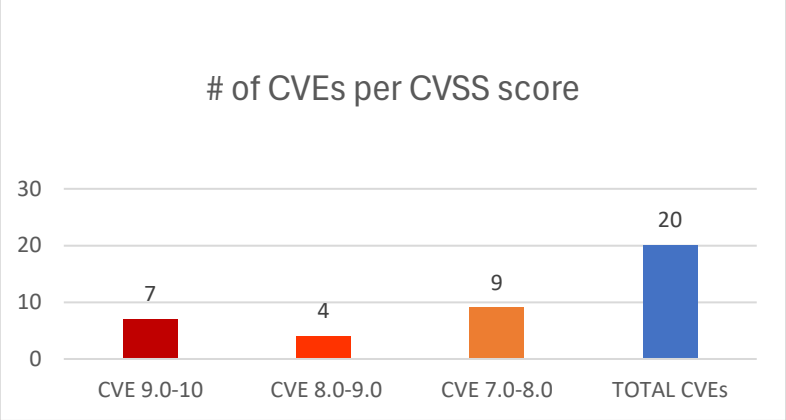
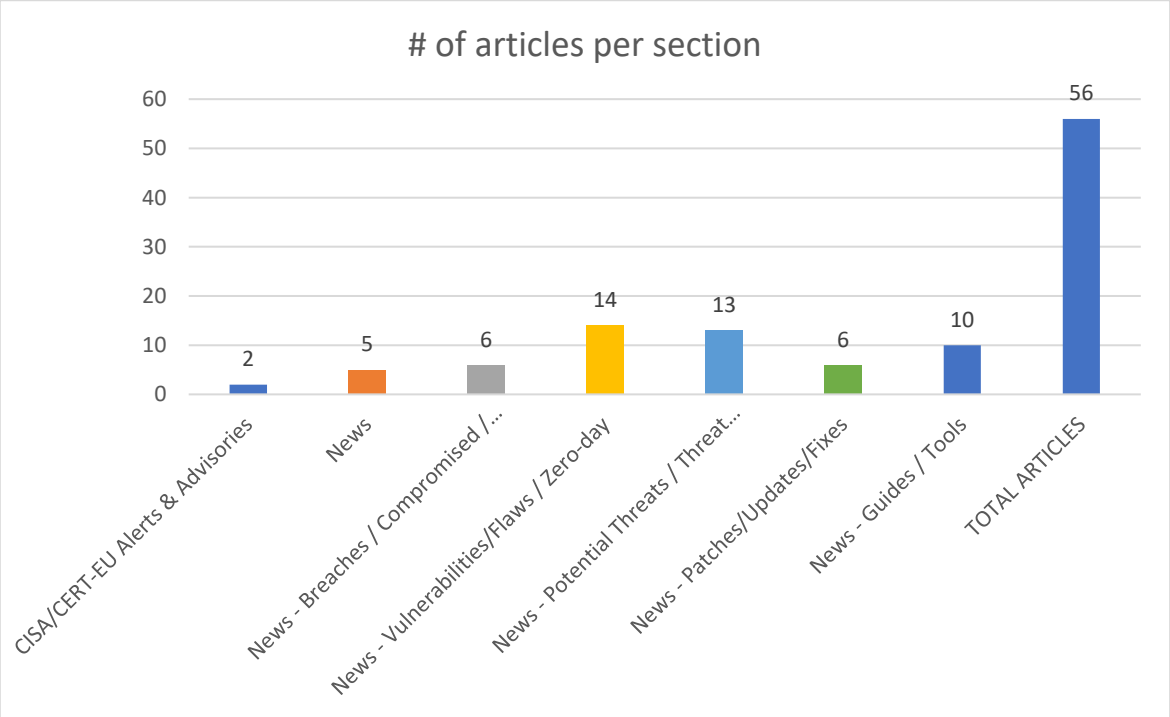
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 21/01/2026 - 23/01/2026





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-2026-24306	9,8	Azure Front Door (AFD)	Improper Access Control		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-24306
https://nvd.nist.gov/vuln/detail/CVE-2026-24061	9,8	telnetd in GNU Inetutils	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	through 2.7	http://www.openwall.com/lists/oss-security/2026/01/22/1 CVE https://www.gnu.org/software/inetutils/ MITRE https://www.openwall.com/lists/oss-security/2026/01/20/2 MITRE https://www.openwall.com/lists/oss-security/2026/01/20/2#:~:text=root@...a%3A~%20USER=' CISA-ADP https://www.openwall.com/lists/oss-security/2026/01/20/8
https://nvd.nist.gov/vuln/detail/CVE-2026-23524	9,8	Laravel Reverb	Deserialization of Untrusted Data	1.6.3 and below	https://cwe.mitre.org/data/definitions/502.html GitHub, Inc. https://github.com/laravel/reverb/commit/9ec26f8ffbb701f84920dd0bb9781a1797591f1a GitHub, Inc. https://github.com/laravel/reverb/releases/tag/v1.7.0 GitHub, Inc. https://github.com/laravel/reverb/security/advisories/GHSA-m27r-m6rx-mhm4 GitHub, Inc. https://laravel.com/docs/12.x/reverb#scaling
https://nvd.nist.gov/vuln/detail/CVE-2026-22793	9,6	5ire	Improper Control of Generation of Code ('Code Injection')	Prior to version 0.15.3	https://github.com/nanbingxyz/5ire/releases/tag/v0.15.3 GitHub, Inc.

					https://github.com/nanbingxyz/5ire/security/advisories/GHSA-wg3x-7c26-97wj
https://nvd.nist.gov/vuln/detail/CVE-2026-24042	9,4	Appsmith	Missing Authorization	1.94 and below	https://github.com/appsmithorg/appsmith/security/advisories/GHSA-j9qq-4fj9-9883
https://nvd.nist.gov/vuln/detail/CVE-2026-24307	9,3	M365 Copilot	Improper Validation of Specified Type of Input		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-24307
https://nvd.nist.gov/vuln/detail/CVE-2026-24002	9,0	Grist	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	1.7.9 and up	https://github.com/gristlabs/grist-core/security/advisories/GHSA-7xvx-8pf2-pv5g GitHub, Inc. https://support.getgrist.com/self-managed/#how-do-i-sandbox-documents
https://nvd.nist.gov/vuln/detail/CVE-2026-22807	8,8	vLLM	Improper Control of Generation of Code ('Code Injection')	0.10.1 and prior to version 0.14.0	https://github.com/vllm-project/vllm/commit/78d13ea9de4b1ce5e4d8a5af9738fea71fb024e5 GitHub, Inc. https://github.com/vllm-project/vllm/pull/32194 GitHub, Inc. https://github.com/vllm-project/vllm/releases/tag/v0.14.0 GitHub, Inc. https://github.com/vllm-project/vllm/security/advisories/GHSA-2pc9-4j83-qjmr
https://nvd.nist.gov/vuln/detail/CVE-2026-24038	8,1	Horilla	Improper Authentication	1.4.0	https://github.com/horilla-opensource/horilla/releases/tag/1.5.0 GitHub, Inc. https://github.com/horilla-opensource/horilla/security/advisories/GHSA-hqpv-ff5v-3hwf
https://nvd.nist.gov/vuln/detail/CVE-2026-24009	8,1	Docling Core (or docling-core)	Deserialization of Untrusted Data	2.21.0 and prior to version 2.48.4	https://github.com/advisories/GHSA-8q59-q68h-6hv4 GitHub, Inc. https://github.com/docling-project/docling-core/commit/3e8d628eeeae50f0f8f239c8c7fea773d065d8

					0c GitHub, Inc. https://github.com/docling-project/docling-core/issues/482 GitHub, Inc. https://github.com/docling-project/docling-core/releases/tag/v2.48.4 GitHub, Inc. https://github.com/docling-project/docling-core/security/advisories/GHSA-vqxf-v2gg-x3hc
https://nvd.nist.gov/vuln/detail/CVE-2026-24129	8,0	Runtipi	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	3.7.0	https://github.com/runtipi/runtipi/commit/c3aa948885554a370d374692158a3bfe1cfdc85a GitHub, Inc. https://github.com/runtipi/runtipi/releases/tag/v4.7.0 GitHub, Inc. https://github.com/runtipi/runtipi/security/advisories/GHSA-vrgf-rcj5-6gv9
https://nvd.nist.gov/vuln/detail/CVE-2026-24016	7,8	The installer of ServerView Agents for Windows	Uncontrolled Search Path Element		https://jvn.jp/en/jp/JVN65211823/ JPCERT/CC https://www.fsastech.com/ja-jp/resources/security/2026/0121.html
https://nvd.nist.gov/vuln/detail/CVE-2026-24138	7,5	FOG	Server-Side Request Forgery (SSRF)	1.5.10.1754	https://github.com/FOGProject/fogproject/security/advisories/GHSA-79xw-c2qx-g7xj
https://nvd.nist.gov/vuln/detail/CVE-2026-23962	7,5	Mastodon	Allocation of Resources Without Limits or Throttling	before v4.3.18, v4.4.12, and v4.5.5	https://github.com/mastodon/mastodon/releases/tag/v4.3.18 GitHub, Inc. https://github.com/mastodon/mastodon/releases/tag/v4.4.12 GitHub, Inc. https://github.com/mastodon/mastodon/releases/tag/v4.5.5 GitHub, Inc. https://github.com/mastodon/mastodon/security/advisories/GHSA-gg8q-rcg7-p79g
https://nvd.nist.gov/vuln/detail/CVE-2026-24006	7,5	Seroval	Allocation of Resources Without Limits or Throttling	1.4.0 and below	https://github.com/lxsmnsyc/seroval/commit/ce9408ebc87312fcad345a73c172212f2a798060 GitHub, Inc.

					https://github.com/lxsmnsyc/seroval/security/advisories/GHSA-3j22-8qj3-26mx
https://nvd.nist.gov/vuln/detail/CVE-2026-23988	7,3	Rufus	Time-of-check Time-of-use (TOCTOU) Race Condition	4.11 and below	https://github.com/pbatard/rufus/commit/460cc5768aa45be07941b9e4ebc9bee02d282873 GitHub, Inc. https://github.com/pbatard/rufus/releases/tag/v4.12_BETA GitHub, Inc. https://github.com/pbatard/rufus/security/advisories/GHSA-hcx5-hrhj-xhq9
https://nvd.nist.gov/vuln/detail/CVE-2026-23699	7,2	AP180 series	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	AP_RGOS 11.9(4)B1P8	https://jvn.jp/en/jp/JVN86850670/ JPCERT/CC https://www.ruijie.co.jp/products/rg-ap180-pe_p432111650928590848.html#productDocument
https://nvd.nist.gov/vuln/detail/CVE-2026-24049	7,1	wheel	Incorrect Permission Assignment for Critical Resource	0.46.1 and below	https://github.com/pypa/wheel/commit/7a7d2de96b22a9adf9208afcc9547e1001569fef GitHub, Inc. https://github.com/pypa/wheel/releases/tag/0.46.2 GitHub, Inc. https://github.com/pypa/wheel/security/advisories/GHSA-8rrh-rw8j-w5fx
https://nvd.nist.gov/vuln/detail/CVE-2026-24046	7,1	Backstage	Improper Link Resolution Before File Access ('Link Following')		https://github.com/backstage/backstage/commit/c641c147ab371a9a8a2f5f67fdb7cb9c97ef345d GitHub, Inc. https://github.com/backstage/backstage/security/advisories/GHSA-rq6q-wr2q-7pgp
https://nvd.nist.gov/vuln/detail/CVE-2026-22444	7,1	The "create core" API of Apache Solr	Improper Input Validation	8.6 through 9.10.0	http://www.openwall.com/lists/oss-security/2026/01/20/5 CVE https://lists.apache.org/thread/qkrb9dd4xrlqmmq73lrhkbfkttto2d1m

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-2026-20045 Cisco Unified Communications Products Code Injection Vulnerability**	**https://www.cisa.gov/news-events/alerts/2026/01/21/cisa-adds-one-known-exploited-vulnerability-catalog**
CISA Adds Four Known Exploited Vulnerabilities to Catalog	▪ CVE-2025-31125 Vite Vitejs Improper Access Control Vulnerability ▪ CVE-2025-34026 Versa Concerto Improper Authentication Vulnerability ▪ CVE-2025-54313 Prettier eslint-config-prettier Embedded Malicious Code Vulnerability ▪ CVE-2025-68645 Synacor Zimbra Collaboration Suite (ZCS) PHP Remote File Inclusion Vulnerability	https://www.cisa.gov/news-events/alerts/2026/01/22/cisa-adds-four-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
EU Unveils Cybersecurity Overhaul with Proposed Update to Cybersecurity Act	https://www.infosecurity-magazine.com/news/eu-unveils-cybersecurity-act-2/
Experts Welcome Global Cybersecurity Vulnerability Enumeration Launch	https://www.infosecurity-magazine.com/news/global-cybersecurity-vulnerability/
Risk of AI Model Collapse to Drive Zero Trust Data Governance, Gartner Says	https://www.infosecurity-magazine.com/news/ai-model-collapse-zero-trust-data/
CISA Releases BRICKSTORM Malware Analysis with New YARA Rules for VMware vSphere	https://cybersecuritynews.com/cisa-releases-brickstorm-malware-report/
Microsoft Teams External Domain Anomalies Allow Defenders to Detect Attackers at Earliest	https://cybersecuritynews.com/microsoft-teams-external-domain-anomalies/

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
Everest Ransomware Claims McDonalds India Breach Involving Customer Data	https://hackread.com/everest-ransomware-mcdonalds-india-breach-customer-data/?&web_view=true
Over 160,000 Companies Notify Regulators of GDPR Breaches	https://www.infosecurity-magazine.com/news/160000-companies-regulator-gdpr/
Peruvian Loan Scam Harvests Cards and PINs via Fake Applications	https://www.infosecurity-magazine.com/news/loan-scam-harvests-cards-pins/
Chainlit AI framework bugs let hackers breach cloud environments	https://www.bleepingcomputer.com/news/security/chainlit-ai-framework-bugs-let-hackers-breach-cloud-environments/
Alleged Ransomware Attack on Apple's Second-Largest Manufacturer Luxshare – Confidential Data Exposed	https://cybersecuritynews.com/luxshare-data-exposed/
Hackers exploit security testing apps to breach Fortune 500 firms	https://www.bleepingcomputer.com/news/security/hackers-exploit-security-testing-apps-to-breach-fortune-500-firms/?&web_view=true

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
Automated FortiGate Attacks Exploit FortiCloud SSO to Alter Firewall Configurations	https://thehackernews.com/2026/01/automated-fortigate-attacks-exploit.html
CERT/CC Warns binary-parser Bug Allows Node.js Privilege-Level Code Execution	https://thehackernews.com/2026/01/certcc-warns-binary-parser-bug-allows.html
Chainlit AI Framework Flaws Enable Data Theft via File Read and SSRF Bugs	https://thehackernews.com/2026/01/chainlit-ai-framework-flaws-enable-data.html
BIND 9 Vulnerability Allow Attackers to Crash Server by Sending Malicious Records	https://cybersecuritynews.com/bind-9-vulnerability/
New Multi-Stage Windows Malware Disables Microsoft Defender Before Dropping Malicious Payloads	https://cybersecuritynews.com/new-multi-stage-windows-malware-disables-microsoft-defender/
Critical Vulnerability in Binary-Parser Library for Node.js Allows Malicious Code injection	https://cybersecuritynews.com/node-js-binary-parser-library-vulnerability/
Critical Oracle WebLogic Server Proxy Vulnerability Lets Attackers Compromise the Server	https://cybersecuritynews.com/oracle-weblogic-server-proxy-vulnerability/
Azure Private Endpoint Deployments Exposes Azure Resources to DoS Attack	https://cybersecuritynews.com/azure-private-endpoint-exposes-azure-resources/

Critical GNU InetUtils Vulnerability Allows Unauthenticated Root Access Via "-f root"	https://cybersecuritynews.com/gnu-inetutils-vulnerability/
Multiple 0-day Vulnerabilities in Anthropic Git MCP Server Enables Code Execution	https://cybersecuritynews.com/anthropic-git-mcp-server-vulnerabilities/
NVIDIA NSIGHT Graphics for Linux Vulnerability Allows Code Execution Attacks	https://cybersecuritynews.com/nvidia-nsight-graphics-linux-vulnerability/
Multiple GitLab Vulnerabilities Enables 2FA Bypass and DoS Attacks	https://cybersecuritynews.com/gitlab-vulnerabilities-enables-2fa-bypass-and-dos-attacks/
Critical Appsmith Flaw Enables Account Takeovers	https://www.infosecurity-magazine.com/news/appsmith-flaw-account-takeovers/
RealHomes CRM Plugin Flaw Affected 30,000 WordPress Sites	https://www.infosecurity-magazine.com/news/realhomes-crm-plugin-flaw/

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
Cisco Fixes Actively Exploited Zero-Day CVE-2026-20045 in Unified CM and Webex	https://thehackernews.com/2026/01/cisco-fixes-actively-exploited-zero-day.html
Zoom and GitLab Release Security Updates Fixing RCE, DoS, and 2FA Bypass Flaws	https://thehackernews.com/2026/01/zoom-and-gitlab-release-security.html
Atlassian, GitLab, Zoom Release Security Patches	https://www.securityweek.com/atlassian-gitlab-zoom-release-security-patches/
Oracle's First 2026 CPU Delivers 337 New Security Patches	https://www.securityweek.com/oracles-first-2026-cpu-delivers-337-new-security-patches/
Google Chrome 144 Update Patches High-Severity V8 Vulnerability	https://cybersecuritynews.com/chrome-144-patches-v8-vulnerability/
New Windows 11 KB5074109 Update Breaks Systems – Microsoft Asks Users to Remove Update	https://cybersecuritynews.com/windows-11-update-breaks-systems/

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
VoidLink Linux Malware Was Built Using an AI Agent, Researchers Reveal	https://www.infosecurity-magazine.com/news/voidlink-linux-malware-built-using/
Hackers Weaponized 2,500+ Security Tools to Terminate Endpoint Protection Before Deploying Ransomware	**https://cybersecuritynews.com/hackers-weaponized-2500-security-tools/**
Attackers Leverages LinkedIn to Deliver Remote Access Trojan Targeting Corporate Environments	https://cybersecuritynews.com/attackers-leverages-linkedin-to-deliver-remote-access-trojan/
Hackers Extensively Abuses Visual Studio Code to Execute Malicious Payloads on Victim System	https://cybersecuritynews.com/hackers-extensively-abuses-visual-studio-code/

Beware of Weaponized Shipping Documents that Deliver Remcos RAT with a Wide Range of Capabilities	https://cybersecuritynews.com/beware-of-weaponized-shipping-documents-that-deliver-remcos-rat/
Threat Actors Hiding stealthy PURELOGS Payload Within a Weaponized PNG File	https://cybersecuritynews.com/threat-actors-hiding-stealthy-purelogs-payload/
LastPass Warns of Fake Maintenance Message Tracking Users to Steal Master Passwords	https://cybersecuritynews.com/lastpass-warns-of-fake-maintenance-message/
New PixelCode Attack Smuggles Malware via Image Pixel Encoding	https://cybersecuritynews.com/pixelcode-attack/
ErrTraffic Fueling ClickFix by Breaking the Page Visually and Turns Attack to Glitch-Fix	https://cybersecuritynews.com/errtraffic-fueling-clickfix-by-breaking/
New ClearFake Campaign Leveraging Proxy Execution to Run PowerShell Commands via Trusted Window Feature	https://cybersecuritynews.com/new-clearfake-campaign-leveraging-proxy-execution/
New Osiris Ransomware Using Wide Range of Living off the Land and Dual-use Tools in Attacks	https://cybersecuritynews.com/new-osiris-ransomware-using-wide-range-of-tools/
SmarterMail auth bypass flaw now exploited to hijack admin accounts	https://www.bleepingcomputer.com/news/security/smartermail-auth-bypass-flaw-now-exploited-to-hijack-admin-accounts/
Critical GNU InetUtils telnetd Flaw Lets Attackers Bypass Login and Gain Root Access	https://thehackernews.com/2026/01/critical-gnu-inetutils-telnetd-flaw.html

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/
15 Best Remote Monitoring Tools – 2025	https://cybersecuritynews.com/best-remote-monitoring-tools/
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/

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/