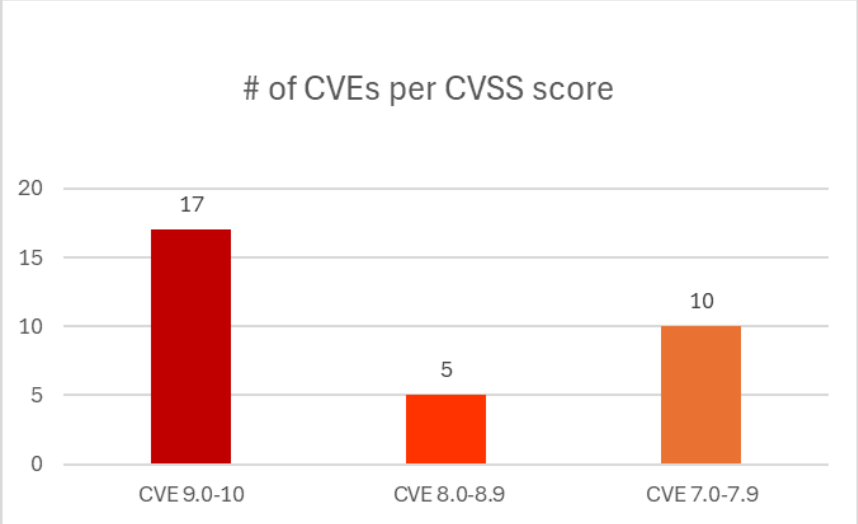
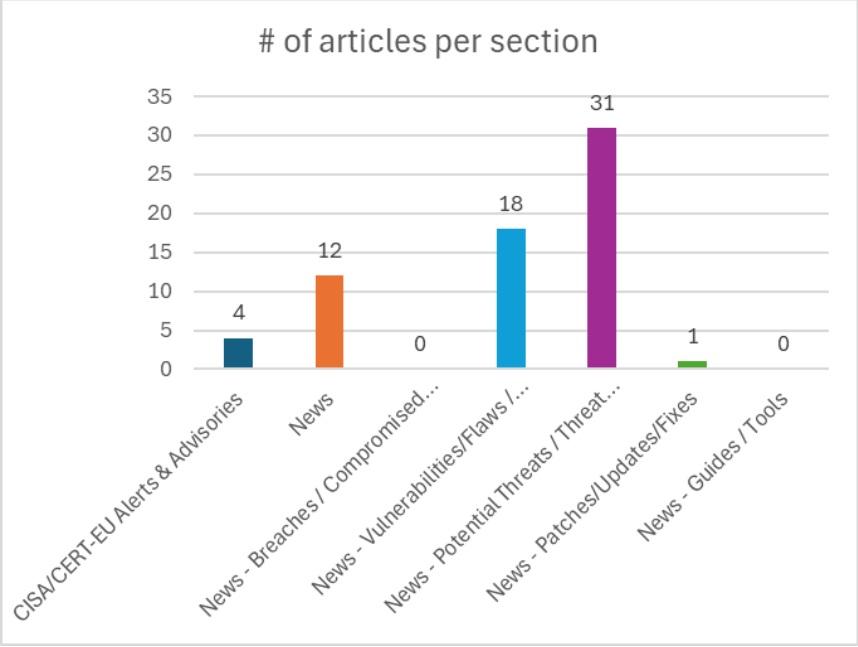
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 18/03/2026 - 20/03/2026





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)	CVSSv 3	Προϊόν/Υ-πηρεσία	Τύπος Ευπά-θειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2026-22557	**10,0**	UniFi Network Application	Improper Limitation of a Pathname to a Re-stricted Di-rectory ('Path Traversal')		https://community.ui.com/releases/Security-Advisory-Bulletin-062-062/c29719c0-405e-4d4a-8f26-e343e99f931b
https://nvd.nist.gov/vuln/de-tail/CVE-2026-30836	**10,0**	Step CA	Improper Authenticati on	Step CA is an online certificate authority for secure, auto-mated certificate management for DevOps. Versions 0.30.0-rc6 and below	https://github.com/smallstep/certificates/commit/e6da031d5125cfd99fe9a26f74bb41e4dacca4ef https://github.com/smallstep/certificates/releases/tag/v0.30.0-rc7 https://github.com/smallstep/certificates/security/advisories/GHSA-q4r8-xm5f-56gw
https://nvd.nist.gov/vuln/detail/CVE-2026-32169	**10,0**	Azure Cloud Shell	Server-Side Request For-gery (SSRF)		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32169
https://www.cve.org/CVE-Record?id=CVE-2026-20131	**10,0**	Cisco Se-cure Fire-wall Man-agement Center (FMC) Soft-ware	Deserializati on of Untrusted Data		https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh
https://nvd.nist.gov/vuln/detail/CVE-2026-21992	**9,8**	Oracle Identity Manager product of Oracle Fu-sion Middle-ware		Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0	https://www.oracle.com/security-alerts/alert-cve-2026-21992.html

https://nvd.nist.gov/vuln/detail/CVE-2026-31998	**9,8**	OpenClaw	Incorrect Authorization	OpenClaw versions 2026.2.22 and 2026.2.23	https://github.com/openclaw/openclaw/commit/0ee30361b8f6ef3f110f3a7b001da6dd3df96bb5 https://github.com/openclaw/openclaw/commit/7655c0cb3a47d0647cbbf5284e177f90b4b82ddb https://github.com/openclaw/openclaw/security/advisories/GHSA-gw85-xp4q-5gp9 https://www.vulncheck.com/advisories/openclaw-authorization-bypass-in-synology-chat-plugin-via-empty-alloweduserids
https://nvd.nist.gov/vuln/detail/CVE-2026-32038	**9,8**	OpenClaw	Improper Access Control	OpenClaw before 2026.2.24	https://github.com/openclaw/openclaw/security/advisories/GHSA-ww6v-v748-x7g9 https://www.vulncheck.com/advisories/openclaw-sandbox-network-isolation-bypass-via-docker-network-container-parameter
https://nvd.nist.gov/vuln/detail/CVE-2026-32191	**9,8**	Microsoft Bing Images	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32191
https://nvd.nist.gov/vuln/detail/CVE-2026-32194	**9,8**	Microsoft Bing Images	Improper Neutralization of Special Elements used in a Command ('Command Injection')		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32194
https://nvd.nist.gov/vuln/detail/CVE-2026-32865	**9,8**	OPEXUS	Exposure of Sensitive Information to an Unauthorized Actor	OPEXUS eComplaint and eCASE before version 10.1.0.0	https://raw.githubusercontent.com/cisagov/CSAF/develop/csaf_files/IT/white/2025/va-26-077-01.json
https://nvd.nist.gov/vuln/detail/CVE-2026-32985	**9,8**	Xerte Online Toolkits	Missing Authentication for Critical Function	Xerte Online Toolkits versions 3.14	https://packetstorm.news/files/id/216288/ https://xot.xerte.org.uk/
https://nvd.nist.gov/vuln/detail/CVE-2026-31938	**9,6**	jsPDF	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	jsPDF is a library to generate PDFs in JavaScript. Prior to version 4.2.1	https://github.com/parallax/jsPDF/commit/87a40bbd07e6b30575196370670b41f264aa78d7 https://github.com/parallax/jsPDF/releases/tag/v4.2.1 https://github.com/parallax/jsPDF/security/advisories/GHSA-wfv2-pwc8-crg5

https://nvd.nist.gov/vuln/detail/CVE-2026-22732	**9,1**	Spring Security		This issue affects Spring Security: from 5.7.0 through 5.7.21, from 5.8.0 through 5.8.23, from 6.3.0 through 6.3.14, from 6.4.0 through 6.4.14, from 6.5.0 through 6.5.8, from 7.0.0 through 7.0.3	https://spring.io/security/cve-2026-22732
https://nvd.nist.gov/vuln/detail/CVE-2026-30704	**9,1**	The WiFi Extender WDR201A	Hidden Functionality	The WiFi Extender WDR201A (HW V2.1, FW LFMZX28040922V1.02)	https://mstreet97.github.io/security-research/iot/vulnerability-disclosure/cybersecurity/cve/2026/02/18/From-Blackbox-to-Whitebox-Multiple-CVEs-in-a-Consumer-WiFi-Extender.html https://www.made-in-china.com/showroom/yeapook/#:~:text=Established%20in%202015.%2CDistrict%2C%20Shenzhen%2C%20Guangdong%2C%20China
https://nvd.nist.gov/vuln/detail/CVE-2026-32633	**9,1**	Glances	Insufficiently Protected Credentials	Prior to version 4.5.2	https://github.com/nicolargo/glances/commit/879ef8688ffa1630839549751d3c7ef9961d361e https://github.com/nicolargo/glances/releases/tag/v4.5.2 https://github.com/nicolargo/glances/security/advisories/GHSA-r297-p3v4-wp8m
https://nvd.nist.gov/vuln/detail/CVE-2026-32698	**9,1**	OpenProject	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Versions prior to 16.6.9, 17.0.6, 17.1.3, and 17.2.1	https://github.com/opf/openproject/security/advisories/GHSA-jqhf-rf9x-9rhx
https://nvd.nist.gov/vuln/detail/CVE-2026-32703	**9,0**	OpenProject	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	In versions prior to 16.6.9, 17.0.6, 17.1.3, and 17.2.1	https://github.com/opf/openproject/security/advisories/GHSA-p423-72h4-fjvp
https://www.cve.org/CVERecord?id=CVE-2026-20963	**8,8**	Microsoft SharePoint	Deserialization of Untrusted Data		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-20963

https://nvd.nist.gov/vuln/detail/CVE-2026-22731	**8,2**	Spring Boot	Authentication Bypass Using an Alternate Path or Channel	This issue affects Spring Boot: from 4.0 before 4.0.3, from 3.5 before 3.5.11, from 3.4 before 3.4.15. This CVE is similar but not equivalent to CVE-2026-22733, as the conditions for exploit and vulnerable versions are different.	https://spring.io/security/cve-2026-22731
https://nvd.nist.gov/vuln/detail/CVE-2026-22733	**8,2**	Spring Boot	Authentication Bypass Using an Alternate Path or Channel	This issue affects Spring Security: from 4.0.0 through 4.0.3, from 3.5.0 through 3.5.11, from 3.4.0 through 3.4.14, from 3.3.0 through 3.3.17, from 2.7.0 through 2.7.31	https://spring.io/security/cve-2026-22733
https://nvd.nist.gov/vuln/detail/CVE-2026-31898	**8,1**	jsPDF is a library to generate PDFs in JavaScript	Improper Encoding or Escaping of Output	Prior to version 4.2.1	https://github.com/parallax/jsPDF/blob/b1607a9391d4cd65ea7ade25998aea8345ae1be3/src/modules/annotations.js#L193-L208 https://github.com/parallax/jsPDF/commit/4155c4819d5eca284168e51e0e1e81126b4f14b8 https://github.com/parallax/jsPDF/releases/tag/v4.2.1 https://github.com/parallax/jsPDF/security/advisories/GHSA-7x6v-j9x4-qf24
https://nvd.nist.gov/vuln/detail/CVE-2026-32808	**8,1**	pyLoad is a free and open-source download manager written in Python	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Versions before 0.5.0b3.dev97	https://github.com/pyload/pyload/security/advisories/GHSA-7g4m-8hx2-4qh3
https://nvd.nist.gov/vuln/detail/CVE-2026-28461	**7,5**	OpenClaw	Allocation of Resources Without Limits or Throttling	OpenClaw versions prior to 2026.3.1	https://github.com/openclaw/openclaw/security/advisories/GHSA-wr6m-jg37-68xh https://www.vulncheck.com/advisories/openclaw-unbounded-memory-growth-in-zalo-webhook-via-query-string-key-churn
https://nvd.nist.gov/vuln/detail/CVE-2026-30922	**7,5**	pyasn1 is a generic ASN.1 library for Python	Uncontrolled Recursion	Prior to 0.6.3	https://github.com/pyasn1/pyasn1/commit/25ad481c19fdb006e20485ef3fc2e5b3eff30ef0 https://github.com/pyasn1/pyasn1/security/advisories/GHSA-jr27-m4p2-rc6r

https://nvd.nist.gov/vuln/detail/CVE-2026-32875	**7,5**	UltraJSON is a fast JSON encoder and decoder written in pure C with bindings for Python 3.7+	Integer Overflow or Wraparound	Versions 5.10 through 5.11.0	https://github.com/ultrajson/ultrajson/commit/486bd4553dc471a1de11613bc7347a6b318e37ea https://github.com/ultrajson/ultrajson/issues/700 https://github.com/ultrajson/ultrajson/security/advisories/GHSA-c8rr-9gxc-jprv
https://nvd.nist.gov/vuln/detail/CVE-2026-32933	**7,5**	AutoMapper	Uncontrolled Recursion	Versions prior to 15.1.1 and 16.1.1	https://github.com/LuckyPennySoftware/AutoMapper/commit/0afaf1e91648fca1a57512e94dd00a76ee016816 https://github.com/LuckyPennySoftware/AutoMapper/releases/tag/v15.1.1 https://github.com/LuckyPennySoftware/AutoMapper/releases/tag/v16.1.1 https://github.com/LuckyPennySoftware/AutoMapper/security/advisories/GHSA-rvv3-g6hj-g44x
https://nvd.nist.gov/vuln/detail/CVE-2026-32944	**7,5**	Parse Server	Uncontrolled Recursion	Prior to 9.6.0-alpha.21 and 8.6.45	https://github.com/parse-community/parse-server/pull/10202 https://github.com/parse-community/parse-server/pull/10203 https://github.com/parse-community/parse-server/security/advisories/GHSA-9xp9-j92r-p88v
https://nvd.nist.gov/vuln/detail/CVE-2026-33002	**7,5**	Jenkins	Reliance on Reverse DNS Resolution for a Security-Critical Action	Jenkins 2.442 through 2.554 (both inclusive), LTS 2.426.3 through LTS 2.541.2 (both inclusive)	https://www.jenkins.io/security/advisory/2026-03-18/#SECURITY-3674
https://nvd.nist.gov/vuln/detail/CVE-2026-4427	**7,5**	PostgreSQL server	Improper Validation of Array Index	pgproto3	https://access.redhat.com/security/cve/CVE-2026-4427 Red Hat, Inc. https://bugzilla.redhat.com/show_bug.cgi?id=2448626 https://github.com/golang/vulndb/issues/4518 https://github.com/jackc/pgproto3 https://github.com/jackc/pgx/issues/2507 https://securityinfinity.com/research/memory-safety-vulnerabilities-in-go-postgresql-wire-protocol-parsers-pgproto3-pgx
https://nvd.nist.gov/vuln/detail/CVE-2026-4428	**7,4**	AWS-LC	Improper Check for Certificate Revocation	AWS-LC before 1.71.0	https://aws.amazon.com/security/security-bulletins/2026-010-AWS/ https://github.com/aws/aws-lc/releases/tag/v1.71.0
https://nvd.nist.gov/vuln/detail/CVE-2026-3090	**7,2**	Post SMTP	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	The Post SMTP – Complete Email Deliverability and SMTP Solution with Email Logs, Alerts, Backup SMTP & Mobile App plugin for WordPress. in all versions up to, and including, 3.8.0	https://plugins.trac.wordpress.org/browser/post-smtp/trunk/Postman/PostmanEmailLogs.php#L459 https://plugins.trac.wordpress.org/changeset/3484515/ https://www.wordfence.com/threat-intel/vulnerabilities/id/3f8cbbbb-2089-4966-8fd3-da4f76fb2517?source=cve

https://www.cve.org/CVE-Record?id=CVE-2025-66376	**7,2**	Zimbra Collaboration (ZCS)	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting')	Zimbra Collaboration (ZCS) 10 before 10.0.18 and 10.1 before 10.1.13	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories https://wiki.zimbra.com/wiki/Security_Center https://wiki.zimbra.com/wiki/Zimbra_Responsible_Disclosure_Policy https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.13#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.18#Security_Fixes

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-2026-20131 Cisco Secure Firewall Management Center (FMC) Software and Cisco Security Cloud Control (SCC) Firewall Management Deserialization of Untrusted Data Vulnerability	https://www.cisa.gov/news-events/alerts/2026/03/19/cisa-adds-one-known-exploited-vulnerability-catalog
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2026-20963 Microsoft SharePoint Deserialization of Untrusted Data Vulnerability	https://www.cisa.gov/news-events/alerts/2026/03/18/cisa-adds-one-known-exploited-vulnerability-catalog-0
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2025-66376 Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting Vulnerability	https://www.cisa.gov/news-events/alerts/2026/03/18/cisa-adds-one-known-exploited-vulnerability-catalog
CISA Urges Endpoint Management System Hardening After Cyberattack Against US Organization		https://www.cisa.gov/news-events/alerts/2026/03/18/cisa-urges-endpoint-management-system-hardening-after-cyberattack-against-us-organization

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
Authorities Disrupt IoT Botnet Infrastructure Behind Record-Breaking 30 Tbps DDoS Attacks	https://cybersecuritynews.com/authorities-disrupts-iot-botnet/
CISA Urges Organizations to Secure Microsoft Intune Environments Following Stryker Breach	https://cybersecuritynews.com/secure-microsoft-intune-environments/
New iOS Exploit With Advanced iPhone Hacking Tools Attacking Users to Steal Personal Data	https://cybersecuritynews.com/darksword-ios-exploit/
The High Cost of Slow Triage: How to Make Tier 1 the Fastest Layer in Your SOC	https://cybersecuritynews.com/the-high-cost-of-slow-triage-how-to-make-tier-1-the-fastest-layer-in-your-soc/
OpenAI Launches GPT-5.4 Mini and Nano to Provide Answers 2X Faster	https://cybersecuritynews.com/openai-launches-gpt-5-4-mini-and-nano/
UIDAI Launches Bug Bounty Programme to Strengthen Aadhaar Security	https://cybersecuritynews.com/uidai-bug-bounty/
Microsoft to Stop Force Installation of 365 Copilot App on Windows Devices	https://cybersecuritynews.com/microsoft-365-copilot-app-installation/
Microsoft Teams Support Call Leads to Quick Assist Compromise in New Vishing Attack	https://cybersecuritynews.com/microsoft-teams-support-call/
Simple Custom Font Rendering Can Poison ChatGPT, Claude, Gemini, and Other AI Systems	https://cybersecuritynews.com/custom-font-poison-ai-systems/
To Beat Alert Overload, Stop Wasting Time on False Positives	https://cybersecuritynews.com/to-beat-alert-overload-stop-wasting-time-on-false-positives/
Attackers Hijacking Legitimate Websites to Attack Microsoft Teams users	https://cybersecuritynews.com/hijacking-websites-microsoft-teams-users/
Stryker Confirms Destructive Wiper Attack – Tens of Thousands of Devices Wiped	https://cybersecuritynews.com/stryker-wiper-attack/

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

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
CISA Warns of Zimbra Collaboration Suite Vulnerability Exploited in Attacks	https://cybersecuritynews.com/zimbra-vulnerability-exploited-attacks/
Critical Ubiquiti UniFi Vulnerabilities Allow Attackers to Seize Full Control of Underlying Systems	https://cybersecuritynews.com/ubiquiti-unifi-vulnerabilities/
Claude Vulnerabilities Allow Data Exfiltration and User Redirection to Malicious Sites	https://cybersecuritynews.com/claude-vulnerabilities-exfiltrate-sensitive/
CISA Warns of Microsoft SharePoint Vulnerability Exploited in Attacks	https://cybersecuritynews.com/microsoft-sharepoint-vulnerability-exploited/
Cisco Firewall 0-day Vulnerability Exploited in the Wild to Deploy Interlock Ransomware	https://cybersecuritynews.com/cisco-firewall-0-day-ransomware/
Apple WebKit Vulnerability Enables Malicious Web Content Bypass on iOS and macOS	https://cybersecuritynews.com/apple-webkit-vulnerability/
ScreenConnect Vulnerability Allows Hackers to Extract Unique Machine Keys and Hijack Sessions	https://cybersecuritynews.com/screenconnect-vulnerability-machine-keys/
Critical Telnetd Vulnerability Enables Remote Attacker to Execute Arbitrary Code via Port 23	https://cybersecuritynews.com/telnetd-vulnerability-enables-remote-attack/
‘RegPwn’ Windows Registry Vulnerability Enables Full System Access to Attackers	https://cybersecuritynews.com/regpwn-windows-registry-vulnerability/
Critical FortiClient SQL Injection Vulnerability Enables Arbitrary Database Access	https://cybersecuritynews.com/forticlient-sql-injection-vulnerability/
Ubuntu Desktop Systems Vulnerability Enables Attackers to Gain Full Root Access	https://cybersecuritynews.com/ubuntu-desktop-systems-vulnerability/
AWS Bedrock AgentCore Sandbox Bypass Allows Covert C2 Channels and Data Exfiltration	https://cybersecuritynews.com/aws-bedrock-agentcore-sandbox-bypass/
Kubernetes CSI Driver for NFS Vulnerability Lets Attackers Delete or Modify NFS Server Directories	https://cybersecuritynews.com/kubernetes-csi-driver-nfs-vulnerability/
Angular XSS Vulnerability Exposes Thousands of web Applications to XSS Attacks	https://cybersecuritynews.com/angular-xss-vulnerability-xss-attacks/
UK’s Companies House WebFiling Flaw Exposed Private Director Data for Five Months	https://cybersecuritynews.com/uks-companies-house-webfiling-flaw/
CISA Warns of Wing FTP Server Vulnerability Exploited in Attacks	https://cybersecuritynews.com/wing-ftp-server-vulnerability-exploited-2/
CISA Warns of Chrome 0-Day Vulnerabilities Exploited in Attacks	https://cybersecuritynews.com/cisa-chrome-0-day-vulnerabilities/
Researchers Decrypt and Exploit Encrypted Palo Alto Cortex XDR BIOC Rules	https://cybersecuritynews.com/decrypt-and-exploit-cortex-xdr/

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
New Windows 11 25H2/24H2 Update Fixes Bluetooth Devices Visibility Issues	https://cybersecuritynews.com/windows-11-bluetooth-visibility-bug/

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
SILENTCONNECT Uses VBScript, PowerShell and PEB Masquerading to Deploy ScreenConnect	https://cybersecuritynews.com/silentconnect-uses-vbscript-powershell/
Russian APT Exploits Zimbra XSS to Target Ukrainian Government in 'Operation GhostMail'	https://cybersecuritynews.com/russian-apt-exploits-zimbra-xss/
'Vibe-Coded' Malware Campaign Uses Fake Tools, CDNs and File Hosts to Infect Users	https://cybersecuritynews.com/vibe-coded-malware-campaign-uses-fake-tools/
Malicious 'Pyronut' Package Backdoors Telegram Bots With Remote Code Execution	https://cybersecuritynews.com/malicious-pyronut-package-backdoors/
Horabot Banking Trojan Resurfaces in Mexico With Multi-Stage Phishing and Email Worm Tactics	https://cybersecuritynews.com/horabot-banking-trojan-resurfaces-in-mexico/
Backdoored Open VSX Extension Used GitHub Downloader to Deploy RAT and Stealer	https://cybersecuritynews.com/backdoored-open-vsx-extension-used-github-downloader/
Iran-Linked Botnet Exposed After Open Directory Leak Reveals 15-Node Relay Network	https://cybersecuritynews.com/iran-linked-botnet-exposed-after-open-directory-leak/
WaterPlum Deploys New 'StoatWaffle' Malware in VSCode-Based Supply Chain Campaign	https://cybersecuritynews.com/waterplum-deploys-new-stoatwaffle-malware/
New SnappyClient Implant Combines Remote Access, Data Theft and Advanced Evasion	https://cybersecuritynews.com/new-snappyclient-implant-combines/
New Malware Campaigns Turn Network Devices Into DDoS Nodes and Crypto-Mining Bots	https://cybersecuritynews.com/new-malware-campaigns-turn-network-devices/
FancyBear Server Exposure Reveals Stolen Credentials, 2FA Secrets and NATO-Linked Targets	https://cybersecuritynews.com/fancybear-server-exposure-reveals-stolen-credentials/
LeakNet Scales Ransomware Operations With ClickFix Lures and Stealthy Deno Loader	https://cybersecuritynews.com/leaknet-scales-ransomware-operations/
ForceMemo Hijacks GitHub Accounts, Backdoors Hundreds of Python Repos via Force-Push	https://cybersecuritynews.com/forcememo-hijacks-github-accounts/
Iran-Linked Cyber Campaigns Converge With Electronic and Psychological Warfare as Regional Conflict Escalates	https://cybersecuritynews.com/iran-linked-cyber-campaigns-converge-with-electronic/

Vidar Stealer 2.0 Spreads Through Fake Game Cheats Promoted on GitHub and Reddit	https://cybersecuritynews.com/vidar-stealer-2-0-spreads-through-fake-game-cheats/
Malicious Telegram Download Site Pushes Multi-Stage Loader With In-Memory Execution	https://cybersecuritynews.com/malicious-telegram-download-site/
Boggy Serpens Targets Diplomats and Critical Infrastructure in Multi-Wave Espionage Campaign	https://cybersecuritynews.com/boggy-serpens-targets-diplomats/
Attackers Abuse Court Documents, GitHub Payloads to Infect Judicial Targets With COVERT RAT	https://cybersecuritynews.com/attackers-abuse-court-documents-targets-with-covert-rat/
Iranian Cyber Ops Maintain US Network Footholds, Target Cameras for Regional Surveillance	https://cybersecuritynews.com/iranian-cyber-ops-maintain-us-network-footholds/
Google Warns Ransomware Actors Are Shifting Tactics as Profits Fall and Data Theft Rises	https://cybersecuritynews.com/google-warns-ransomware-actors-are-shifting/
Glassworm Hits Popular React Native Packages With Credential-Stealing npm Malware	https://cybersecuritynews.com/glassworm-hits-popular-react-native-packages/
Attackers Use SEO Poisoning and Signed Trojans to Steal VPN Credentials	https://cybersecuritynews.com/attackers-use-seo-poisoning-and-signed-trojans/
6 Malicious Packagist Themes Ship Trojanized jQuery in OphimCMS Supply Chain Attack	https://cybersecuritynews.com/6-malicious-packagist-themes-ship-trojanized-jquery/
Phishers Weaponize Safe Links With Multi-Layered URL Rewriting to Evade Detection	https://cybersecuritynews.com/phishers-weaponize-safe-links-with-multi-layered-url/
New 'Payload' Ransomware Uses Babuk-Style Encryption Against Windows and ESXi Systems	https://cybersecuritynews.com/new-payload-ransomware-uses-babuk-style-encryption/
Malicious npm Packages Deliver PylangGhost RAT in New Software Supply Chain Campaign	https://cybersecuritynews.com/malicious-npm-packages-deliver-pylangghost-rat/
Phishers Abuse LiveChat Support Tools to Steal Sensitive Data in New SaaS-Based Attack Tactic	https://cybersecuritynews.com/phishers-abuse-livechat-support-tools/
New CondiBot Variant and 'Monaco' Cryptominer Expand Threats to Network Devices	https://cybersecuritynews.com/new-condibot-variant-and-monaco-cryptominer/
Handala Hack Uses RDP, NetBird, and Parallel Wipers in MOIS-Linked Destructive Intrusions	https://cybersecuritynews.com/handala-hack-uses-rdp/
CamelClone Spy Campaign Abuses Public File-Sharing Sites and Rclone in Government-Focused Attacks	https://cybersecuritynews.com/camelclone-spy-campaign/
RondoDox Botnet Expands to 174 Exploits, Leveraging Residential IP Infrastructure at Scale	https://cybersecuritynews.com/rondodox-botnet-expands/

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/