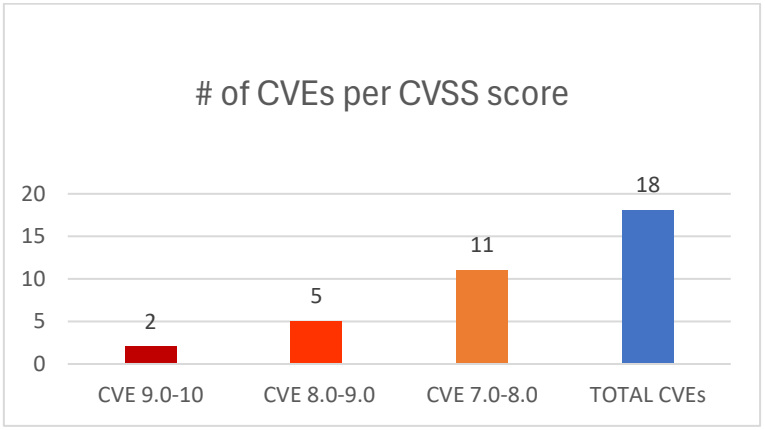
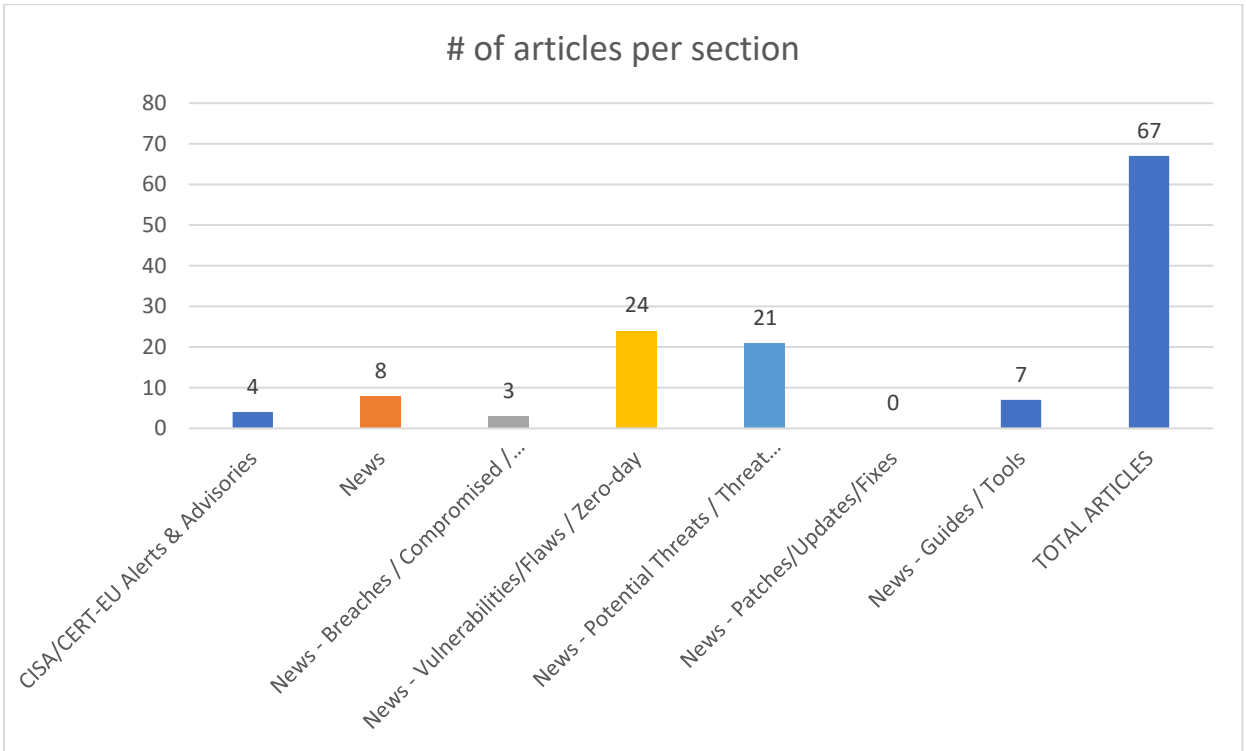
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 12/11/2025 - 14/11/2025





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/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2025-12870	9,8	The a+HRD	Weak Authentication		https://www.chtsecurity.com/news/b97e8337-6b0c-43e8-8e8c-187b7c0e13c2 CVE https://www.twcert.org.tw/en/cp-139-10487-12a32-2.html TWCERT/CC https://www.twcert.org.tw/tw/cp-132-10486-a3459-1.html
https://nvd.nist.gov/vuln/detail/CVE-2025-46608	9,1	Dell Data Lakehouse	Improper Access Control	prior to 1.6.0.0	https://www.dell.com/support/kbdoc/en-us/000390529/dsa-2025-375-security-update-for-dell-data-lakehouse-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2025-46428	8,8	Dell SmartFabric OS10 Software	Improper Neutralization of Special Elements used in a Command ('Command Injection')	prior to 10.6.1.0	https://www.dell.com/support/kbdoc/en-us/000391062/dsa-2025-407-security-update-for-dell-networking-os10-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2025-13042	8,8	V8 in Google Chrome	heap corruption	prior to 142.0.7444.166	https://chromereleases.googleblog.com/2025/11/stable-channel-update-for-desktop_11.html Chrome https://issues.chromium.org/issues/457351015
https://nvd.nist.gov/vuln/detail/CVE-2025-64186	8,7	Evervault	Improper Verification of Cryptographic Signature	prior to 1.3.2	https://github.com/evervault/evervault-go/commit/7c824d289bba11ec0bea46a338023f5b128bbb28 GitHub, Inc. https://github.com/evervault/evervault-go/pull/48 GitHub, Inc. https://github.com/evervault/evervault-go/security/advisories/GHSA-88h9-77c7-p6w4
https://nvd.nist.gov/vuln/detail/CVE-2025-64484	8,5	OAuth2-Proxy	Improper Neutralization of HTTP Headers for Scripting Syntax	prior to 7.13.0	https://datatracker.ietf.org/doc/html/rfc2616#section-4.2 GitHub, Inc. https://datatracker.ietf.org/doc/html/rfc822#section-3.2 GitHub, Inc. https://github.com/oauth2-proxy/oauth2-proxy/security/advisories/GHSA-vjrc-mh2v-45x6 GitHub, Inc. https://github.security.telekom.com/2020/05/smuggling-http-headers-through-reverse-proxies.html GitHub, Inc. https://www.uptimia.com/questions/why-are-http-headers-with-underscores-dropped-by-nginx

https://nvd.nist.gov/vuln/detail/CVE-2025-65001	8,2	Fujitsu fbiosdrv.sys	Out-of-bounds Write	before 2.5.0.0	https://hexaplex.ai MITRE https://security.ts.fujitsu.com/ProductSecurity/content/FsasTech-PSIRT-FTI-FCCL-2025-072319-Security-Notice.pdf
https://nvd.nist.gov/vuln/detail/CVE-2025-64293	**7,6**	Golemiq 0 Day Analytics	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	from n/a through 4.0.0	https://vdp.patchstack.com/database/wordpress/plugin/0-day-analytics/vulnerability/wordpress-0-day-analytics-plugin-4-0-0-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-11795	7,6	Autodesk 3ds Max	Out-of-bounds Write		https://www.autodesk.com/trust/security-advisories/adsk-sa-2025-0023
https://nvd.nist.gov/vuln/detail/CVE-2025-12048	7,5	Lenovo Scanner Pro client	Unrestricted Upload of File with Dangerous Type		https://iknow.lenovo.com.cn/detail/434326
https://nvd.nist.gov/vuln/detail/CVE-2024-47866	7,5	Ceph	Improper Input Validation	up to and including 19.2.3	http://www.openwall.com/lists/oss-security/2025/11/11/3 CVE https://github.com/ceph/ceph/security/advisories/GHSA-mgrm-g92q-f8h8
https://nvd.nist.gov/vuln/detail/CVE-2025-63667	7,5	API endpoints	Improper Access Control	SIMICAM v1.16.41-20250725, KEVIEW v1.14.92-20241120, ASECAM v1.14.10-20240725	https://github.com/Remenis/CVE-2025-63667 MITRE https://github.com/Remenis/Vatilon_evidence/releases/download/Evidence/Vatilon_vulnerability_evidence_2025.zip
https://nvd.nist.gov/vuln/detail/CVE-2025-12903	7,5	The Payment Plugins Braintree For WooCommerce plugin for WordPress	Authorization Bypass Through User-Controlled Key	up to, and including, 3.2.78	https://developer.wordpress.org/rest-api/using-the-rest-api/authentication/ Wordfence https://plugins.trac.wordpress.org/browser/woo-payment-gateway/tags/3.2.78/includes/api/class-wc-braintree-controller-3ds.php#L23 Wordfence https://plugins.trac.wordpress.org/browser/woo-payment-gateway/tags/3.2.78/includes/api/class-wc-braintree-controller-3ds.php#L35 Wordfence https://plugins.trac.wordpress.org/browser/woo-payment-gateway/tags/3.2.78/includes/api/class-wc-braintree-controller-3ds.php#L41 Wordfence https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3392259%40woo-payment-gateway&new=3392259%40woo-payment-gateway&sfp_email=&sfph_mail= Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/89cd5429-39a0-441f-ba69-dea111eae5ed?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-13047	7,5	Bacteriology Laboratory Reporting System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')		https://www.twcert.org.tw/en/cp-139-10499-15678-2.html TWCERT/CC https://www.twcert.org.tw/tw/cp-132-10498-61fa4-1.html
https://nvd.nist.gov/vuln/detail/CVE-2025-12633	**7,5**	The Booking Calendar | Appointment Booking | Bookit plugin for WordPress	Missing Authorization	up to, and including, 2.5.0	https://plugins.trac.wordpress.org/changeset/3393159/bookit/tags/2.5.1/src/Bookit/Gateways/StripeConnect/REST/Return_Endpoint.php?old=3121677&old_path=bookit%2Ftags%2F2.5.0%2Fsrc%2FBookit%2FGateways%2FStripeConnect%2FREST%2FReturn_Endpoint.php Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/2263d356-b2ed-4e16-98ee-b01d4274d1d9?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-8485	**7,3**	Lenovo App Store	Incorrect Default Permissions		https://iknow.lenovo.com.cn/detail/434329
https://nvd.nist.gov/vuln/detail/CVE-2025-11962	**7,3**	DivvyDrive Information Technologies Inc. Digital Corporate Warehouse	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	before v.4.8.2.22	https://www.usom.gov.tr/bildirim/tr-25-0393
https://nvd.nist.gov/vuln/detail/CVE-2025-11994	**7,2**	The Easy Email Subscription plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 1.3	https://plugins.svn.wordpress.org/email-subscription-with-secure-captcha/tags/1.3/simple-email-subscription.php Wordfence https://plugins.svn.wordpress.org/email-subscription-with-secure-captcha/tags/1.3/subscriber-form.php Wordfence https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3388578%40email-subscription-with-secure-captcha&new=3388578%40email-subscription-with-secure-captcha&sfp_email=&sfph_mail= Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/b5bb14c1-8713-4aa1-b50a-53bed07a5f80?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 Releases 18 Industrial Control Systems Advisories	▪ **ICSA-25-317-01** Mitsubishi Electric MELSEC iQ-F Series ▪ **ICSA-25-317-02** AVEVA Application Server IDE ▪ **ICSA-25-317-03** AVEVA Edge ▪ **ICSA-25-317-04** Brightpick Mission Control / Internal Logic Control ▪ **ICSA-25-317-05** Rockwell Automation Verve Asset Manager ▪ **ICSA-25-317-06** Rockwell Automation Studio 5000 Simulation Interface ▪ **ICSA-25-317-07** Rockwell Automation FactoryTalk DataMosaix Private Cloud ▪ **ICSA-25-317-08** General Industrial Controls Lynx+ Gateway ▪ **ICSA-25-317-09** Rockwell Automation FactoryTalk Policy Manager ▪ **ICSA-25-317-10** Rockwell Automation AADvance-Trusted SIS Workstation ▪ **ICSA-25-317-11** Siemens SICAM P850 family and SICAM P855 family ▪ **ICSA-25-317-12** Siemens Spectrum Power 4 ▪ **ICSA-25-317-13** Siemens LOGO! 8 BM Devices ▪ **ICSA-25-317-14** Siemens Solid Edge ▪ **ICSA-25-317-15** Siemens COMOS ▪ **ICSA-25-317-16** Siemens Altair Grid Engine ▪ **ICSA-25-317-17** Siemens Software Center and Solid Edge ▪ **ICSA-25-273-04** Festo Controller CECC-S,-LK,-D Family Firmware (Update A)	**https://www.cisa.gov/news-events/alerts/2025/11/13/cisa-releases-18-industrial-control-systems-advisories**
CISA and Partners Release Advisory Update on Akira Ransomware		**https://www.cisa.gov/news-events/alerts/2025/11/13/cisa-and-partners-release-advisory-update-akira-ransomware**
Update: Implementation Guidance for Emergency Directive on Cisco ASA and Firepower Device Vulnerabilities	CVE-2025-20333 and CVE-2025-20362	https://www.cisa.gov/news-events/alerts/2025/11/12/update-implementation-guidance-emergency-directive-cisco-asa-and-firepower-device-vulnerabilities
CISA Adds Three Known Exploited Vulnerabilities to Catalog	▪ CVE-2025-9242 WatchGuard Firebox Out-of-Bounds Write Vulnerability ▪ CVE-2025-12480 Gladinet Triofox Improper Access Control Vulnerability ▪ CVE-2025-62215 Microsoft Windows Race Condition Vulnerability	https://www.cisa.gov/news-events/alerts/2025/11/12/cisa-adds-three-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 Wave of Steganography Attacks: Hackers Hiding XWorm in PNGs	https://cybersecuritynews.com/steganography-attacks-xworm-in-pngs/
Microsoft Teams New Premium Feature Blocks Screenshots and Recordings During Meeting	https://cybersecuritynews.com/microsoft-teams-new-feature/
Microsoft Defender for O365 New Feature Allows Security Teams to Trigger Automated Investigations	https://cybersecuritynews.com/microsoft-defendero365-new-feature/
How Attackers Turn SVG Files Into Phishing Lures	https://cybersecuritynews.com/how-attackers-turn-svg-files-into-phishing-lures/
CISA Warns WatchGuard Firebox Out-of-Bounds Write Vulnerability Exploited Attacks	https://cybersecuritynews.com/watchguard-firebox-vulnerability-exploited/
Why your Business Need Live Threat Intel from 15k SOCs	https://cybersecuritynews.com/why-your-business-needs-live-threat-intel-from-15k-socs/
Microsoft Investigating Teams Issue that Disables Users from Opening Apps	https://cybersecuritynews.com/microsoft-investigating-teams-issue/
SecureVibes – AI Tool Scans for Vulnerabilities in 11 Languages with Claude AI Agents	https://cybersecuritynews.com/securevibes/

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
Cl0P Ransomware Group Allegedly Claims Breach of Entrust in Oracle 0-Day EBS Hack	https://cybersecuritynews.com/entrust-oracle-0-day-ebs-hack/
Checkout.com Hacked – ShinyHunters Breached Cloud Storage, Company Refuses Ransom	https://cybersecuritynews.com/checkout-com-hacked/
65% of Leading AI Companies Exposes Verified Secrets Including Keys and Tokens on GitHub	https://cybersecuritynews.com/ai-companies-exposes-keys-and-tokens/

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 Fortinet FortiWeb Vulnerability Exploited in the Wild to Create Admin Accounts	https://cybersecuritynews.com/fortinet-fortiweb-vulnerability/
FortiWeb Authentication Bypass Vulnerability Exploited – Script to Detect Vulnerable Appliances	https://cybersecuritynews.com/fortiweb-authentication-vulnerability-exploited/
Multiple GitLab Vulnerabilities Let Attackers Inject Malicious Prompts to Steal Sensitive Data	https://cybersecuritynews.com/gitlab-vulnerabilities-inject-malicious-prompts/
Multiple Kibana Vulnerabilities Enables SSRF and XSS Attacks	https://cybersecuritynews.com/kibana-ssrf-and-xss-vulnerabilities/
Palo Alto PAN-OS Firewall Vulnerability Let Attackers Reboot Firewall by Sending Malicious Packet	https://cybersecuritynews.com/palo-alto-pan-os-firewall-vulnerability/
Critical Dell Data Lakehouse Vulnerability Let Remote Attacker Escalate Privileges	https://cybersecuritynews.com/dell-data-lakehouse-vulnerability/
OpenAI Sora 2 Vulnerability Exposes System Prompts via Audio Transcripts	https://cybersecuritynews.com/openai-sora-2-vulnerability/
CISA Warns of Federal Agencies Not Fully Patching Actively Exploited Cisco ASA or Firepower Devices	https://cybersecuritynews.com/cisa-warns-federal-agencies/
Citrix NetScaler ADC and Gateway Vulnerability Enables Cross-Site Scripting Attacks	https://cybersecuritynews.com/citrix-netscaler-adc-and-gateway-vulnerability/
Multiple Apache OpenOffice Vulnerabilities Leads to Memory Corruption and Unauthorized Content Loading	https://cybersecuritynews.com/apache-openoffice-vulnerabilities/
GitHub Copilot and Visual Studio Vulnerabilities Allow Attacker to Bypass Security Feature	https://cybersecuritynews.com/github-copilot-and-visual-studio-vulnerabilities/
Hackers Actively Exploiting Cisco and Citrix 0-Day in the Wild to Deploy Webshell	https://cybersecuritynews.com/cisco-and-citrix-0-days-exploited/
Tor Browser 15.0.1 Released With Fix for Multiple Security Vulnerabilities	https://cybersecuritynews.com/tor-browser-15-0-1-released/
ChatGPT Hacked Using Custom GPTs Exploiting SSRF Vulnerability to Expose Secrets	https://cybersecuritynews.com/chatgpt-hacked-using-custom-gpts/
Windows Remote Desktop Services Vulnerability Let Attackers Escalate Privileges	https://cybersecuritynews.com/windows-remote-desktop-services-flaw/
Chrome Patches High-severity Implementation Vulnerability in V8 JavaScript engine	https://cybersecuritynews.com/chrome-security-update-patch-v8-engine/
Windows Kernel 0-day Vulnerability Actively Exploited in the Wild to Escalate Privilege	https://cybersecuritynews.com/windows-kernel-0%e2%80%91day-vulnerability/
Microsoft November 2025 Patch Tuesday – 63 Vulnerabilities, Including 1 Zero-Day Fixed	https://cybersecuritynews.com/microsoft-november-2025-patch-tuesday/
Firefox Releases Security Update to Fix Multiple Vulnerabilities Allowing Arbitrary Code Execution	https://cybersecuritynews.com/firefox-145/
Ivanti Endpoint Manager Vulnerabilities Let Attackers Write Arbitrary Files to Disk	https://cybersecuritynews.com/ivanti-endpoint-manager-vulnerabilities/
Synology BeeStation 0-Day Vulnerability Let Remote Attackers Execute Arbitrary Code	https://cybersecuritynews.com/synology-beestation-0-day-vulnerability/

Zoom Workplace for Windows Vulnerability Allow Users to Escalate Privilege	https://cybersecuritynews.com/zoom-workplace-for-windows-vulnerability/
WatchGuard Firebox Firewall Vulnerability Let Attackers Gain Unauthorized SSH Access	https://cybersecuritynews.com/watchguard-firebox-firewall-vulnerability/
CISA Warns of Samsung Mobile Devices 0-Day RCE Vulnerability Exploited in Attacks	https://cybersecuritynews.com/samsung-0-day-rce-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
Kraken Cross-Platform Ransomware Attacking Windows, Linux, and VMware ESXi Systems in Enterprise Environments	https://cybersecuritynews.com/kraken-attacking-windows-linux-and-vmware-esxi-systems/
New ClickFix Attack Targeting Windows and macOS Users to Deploy Infostealer Malware	https://cybersecuritynews.com/new-clickfix-attack-targeting-windows-and-macos-users/
Android Photo Frames App Downloads Malware, Giving Hackers Control of The Device Without User Interaction	https://cybersecuritynews.com/android-photo-frames-app-downloads-malware/
Beware of Fake Bitcoin Tool That Hides DarkComet RAT Malware With it	https://cybersecuritynews.com/beware-of-fake-bitcoin-tool-that-hides-darkcomet/
Hackers Exploiting RMM Tools LogMeIn and PDQ Connect to Deploy Malware as a Normal Program	https://cybersecuritynews.com/hackers-exploiting-rmm-tools-logmein-and-pdq-connect/
Google Sues ‘Lighthouse’ Phishing-as-a-service Kit Behind Massive Phishing Attacks	https://cybersecuritynews.com/google-sues-lighthouse-phishing-as-a-service-kit/
MastaStealer Weaponizes Windows LNK Files, Executes PowerShell Command, and Evades Defender	https://cybersecuritynews.com/mastastealer-weaponizes-windows-lnk-files/
English-Speaking Cybercriminal Ecosystem ‘The COM’ Drives a Wide Spectrum of Cyberattacks	https://cybersecuritynews.com/english-speaking-cybercriminal-ecosystem-the-com/
New ClickFix Attack Tricks Users with ‘Fake OS Update’ to Execute Malicious Commands	https://cybersecuritynews.com/clickfix-attack-fake-os-update/
Microsoft SQL Server Vulnerability Let Attackers Escalate Privileges	https://cybersecuritynews.com/microsoft-sql-server-vulnerability/
New Phishing Attack Targeting iPhone Owners Who’ve Lost Their Devices	https://cybersecuritynews.com/new-phishing-attack-targeting-iphone-owners/

Massive Phishing Attack Impersonate as Travel Brands Attacking Users with 4,300 Malicious Domains	https://cybersecuritynews.com/massive-phishing-attack-impersonate-as-travel-brands/
Beware of Malicious Steam Cleanup Tool Attack Windows Machines to Deploy Backdoor Malware	https://cybersecuritynews.com/malicious-steam-cleanup-tool-attack-windows-machines/
APT-C-08 Hackers Exploiting WinRAR Vulnerability to Attack Government Organizations	https://cybersecuritynews.com/apt-c-08-hackers-exploiting-winrar-vulnerability/
New Phishing Attack Leverages Popular Brands to Harvest Login Credentials	https://cybersecuritynews.com/new-phishing-attack-leverages-popular-brands/
Hackers Weaponize AppleScript to Creatively Deliver macOS Malware Mimic as Zoom/Teams Updates	https://cybersecuritynews.com/hackers-weaponize-applescript/
Authentication Coercion Attack Tricks Windows Machines into Revealing Credentials to Attack-controlled Servers	https://cybersecuritynews.com/authentication-coercion-attack-tricks-windows-machines/
New Quantum Route Redirect Tool Lets Attackers Launch One-Click Phishing Attacks on Microsoft 365 Users	https://cybersecuritynews.com/new-quantum-route-redirect-tool/
Beware of Security Alert-Themed Malicious Emails that Steal Your Email Logins	https://cybersecuritynews.com/beware-of-security-alert-themed-malicious-emails/
Threat Actors Attacking Outlook and Google Bypassing Traditional Email Defenses	https://cybersecuritynews.com/threat-actors-attacking-outlook/
New VanHelsing Ransomware RaaS Model Attacking Windows, Linux, BSD, ARM, and ESXi Systems	https://cybersecuritynews.com/new-vanhelsing-ransomware-raas-model/

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/

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/