NATIONAL CYBERSECURITY AUTHORITY GR

CVEs Alerts

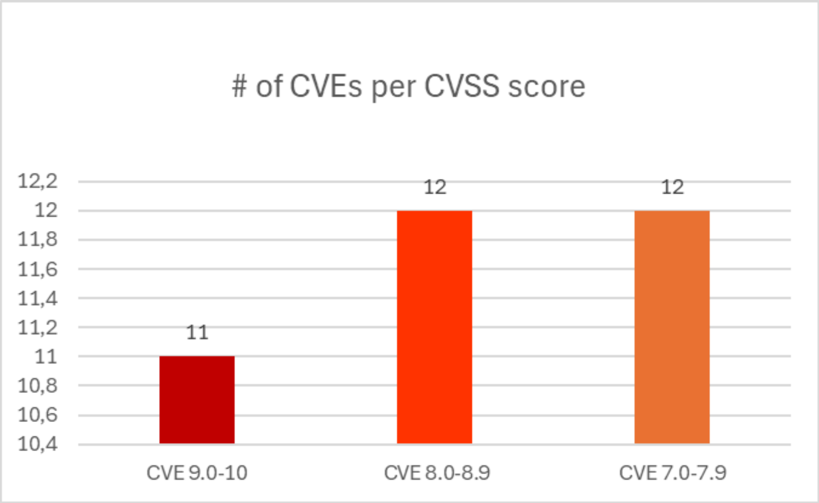
CVEs, CISA/CERT-EU Alerts Advisories & News

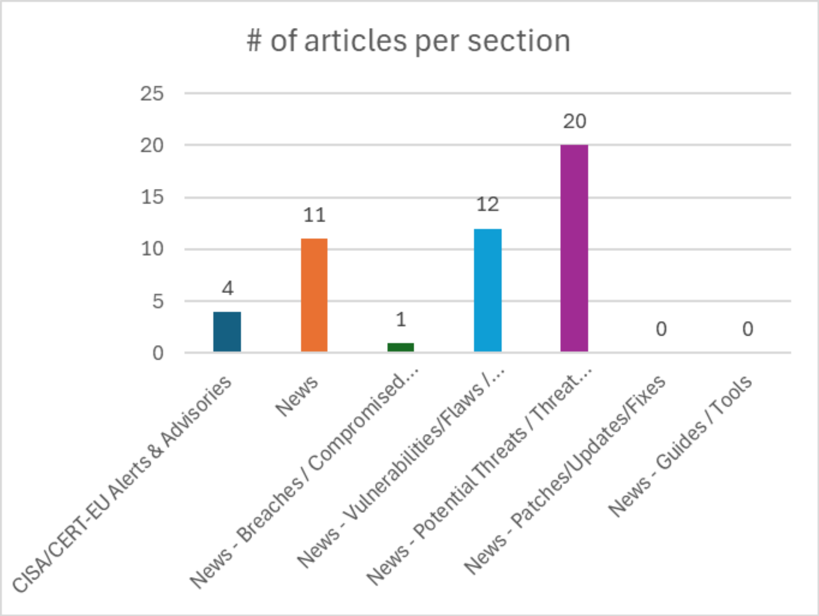
Newsletter on system vulnerabilities and cybersecurity news

Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 23/01/2026 - 27/01/2026





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)	CVSS v3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2016-15057	9,9	Apache Continuum	Improper Neutralization of Special Elements used in a Command ('Command Injection')		http://www.openwall.com/lists/oss-security/2026/01/26/1 https://lists.apache.org/thread/hbvf1ztqw2kv51khvzm5nk3mml3nm4z1
https://nvd.nist.gov/vuln/detail/CVE-2025-70982	9,9	SpringBlade	Improper Access Control	v4.5.0	https://gist.github.com/old6ma/ea60151aa40ddc1cfb51fbaa0c173117 https://github.com/chillzhuang/SpringBlade https://github.com/chillzhuang/SpringBlade/issues/34
https://nvd.nist.gov/vuln/detail/CVE-2025-70457	9,8	Sourcecodester Modern Image Gallery App	Unrestricted Upload of File with Dangerous Type	Sourcecodester Modern Image Gallery App v1.0	https://github.com/ismaildawoodjee/vulnerability-research/security/advisories/GHSA-8xq6-hjhw-4983 https://www.sourcecodester.com/php/18572/modern-image-gallery-app-using-php-and-mysql-source-code.html
https://nvd.nist.gov/vuln/detail/CVE-2026-1364	9,8	JNC (IAQS and I6)	Missing Authentication for Critical Function		https://www.twcert.org.tw/en/cp-139-10653-117a1-2.html https://www.twcert.org.tw/tw/cp-132-10652-4cdca-1.html
https://nvd.nist.gov/vuln/detail/CVE-2026-22709	9,8	vm2	Improper Control of Generation of Code ('Code Injection')	In vm2 prior to version 3.10.2	https://github.com/patriksimek/vm2/commit/4b009c2d4b1131c01810c1205e641d614c322a29 https://github.com/patriksimek/vm2/releases/tag/v3.10.2 https://github.com/patriksimek/vm2/security/advisories/GHSA-99p7-6v5w-7xg8
https://nvd.nist.gov/vuln/detail/CVE-2026-24531	9,8	PHP Remote File Inclusion	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusio	from n/a through <= 2.3	https://patchstack.com/database/Wordpress/Theme/prowess/vulnerability/wordpress-prowess-theme-2-3-local-file-inclusion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-52024	9,4	Aptsys POS Platform Web Services	Missing Authentication for Critical Function		http://aptsys.com https://gist.github.com/ReverseThatApp/4a6be2b9b2ba39d38c35c8753e0afd39

https://nvd.nist.gov/vuln/detail/CVE-2025-59090	9,3	exos 9300 server	Missing Authentication for Critical Function		https://r.sec-consult.com/dkexos https://r.sec-consult.com/dormakaba https://www.dormakabagroup.com/en/security-advisories
https://nvd.nist.gov/vuln/detail/CVE-2026-24399	9,3	ChatterMate	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	In versions 1.0.8 and below	https://github.com/chattermate/chattermate.chat/commit/ff3398031abb97ae28546eaf993fed3619eaffdd https://github.com/chattermate/chattermate.chat/releases/tag/v1.0.9 https://github.com/chattermate/chattermate.chat/security/advisories/GHSA-72p3-w95w-q3j4
https://nvd.nist.gov/vuln/detail/CVE-2026-24436	9,2	Shenzhen Tenda W30E	Improper Restriction of Excessive Authentication Attempts	firmware versions up to and including V16.01.0.19(5037)	https://www.tendacn.com/product/W30E https://www.vulncheck.com/advisories/tenda-w30e-v2-lacks-rate-limiting-on-authentication
https://nvd.nist.gov/vuln/detail/CVE-2025-66719	9,1	Free5gc NRF	Incorrect Authorization	Free5gc NRF 1.4.0	https://github.com/free5gc/free5gc/issues/736 https://github.com/free5gc/nrf/pull/73
https://nvd.nist.gov/vuln/detail/CVE-2025-30248	8,9	Western Digital	Uncontrolled Search Path Element	in Western Digital WD Discovery 5.2.730 on Windows	https://www.westerndigital.com/support/product-security/wdc-25008-wd-discovery-desktop-app-version-5-3
https://nvd.nist.gov/vuln/detail/CVE-2021-47903	8,8	LiteSpeed Web Server	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	LiteSpeed Web Server Enterprise 5.4.11	https://www.exploit-db.com/exploits/49523 https://www.litespeedtech.com/ https://www.litespeedtech.com/products https://www.vulncheck.com/advisories/litespeed-web-server-enterprise-command-injection
https://nvd.nist.gov/vuln/detail/CVE-2025-67847	8,8	Moodle	Improper Control of Generation of Code ('Code Injection')		https://access.redhat.com/security/cve/CVE-2025-67847
https://nvd.nist.gov/vuln/detail/CVE-2026-1420	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda AC23 16.03.07.52	https://github.com/xyh4ck/iot_poc/blob/main/Tenda%20AC23_Buffer_Overflow_WifiExtraSet/Tenda%20AC23_Buffer_Overflow_WifiExtraSet.md https://github.com/xyh4ck/iot_poc/blob/main/Tenda%20AC23_Buffer_Overflow_WifiExtraSet/Tenda%20AC23_Buffer_Overflow_WifiExtraSet.md#poc https://vuldb.com/?ctiid.342836 https://vuldb.com/?id.342836

					https://vuldb.com/?submit.736559 https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-22273	8,8	Dell	Use of Default Credentials	versions 3.8.1.0 through 3.8.1.7	https://www.dell.com/support/kbdoc/en-us/000415880/dsa-2026-047-security-update-for-dell-ecs-and-objectscale-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2026-24532	8,8	SiteLock Security	Missing Authorization	from n/a through <= 5.0.2	https://patchstack.com/database/Wordpress/Plugin/sitelock/vulnerability/wordpress-sitelock-security-plugin-5-0-2-broken-access-control-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-24534	8,8	uPress Booter	Missing Authorization	from n/a through <= 1.5.7	https://patchstack.com/database/Wordpress/Plugin/booter-bots-crawlers-manager/vulnerability/wordpress-booter-plugin-1-5-7-broken-access-control-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-24572	8,8	Nelio Software	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	from n/a through <= 4.1.0	https://patchstack.com/database/Wordpress/Plugin/nelio-content/vulnerability/wordpress-nelio-content-plugin-4-1-0-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-24486	8,6	Python-Multipart	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Prior to version 0.0.22	https://github.com/Kludex/python-multipart/commit/9433f4bbc9652bdde82bbe380984e32f8cfc89c4 https://github.com/Kludex/python-multipart/releases/tag/0.0.22 https://github.com/Kludex/python-multipart/security/advisories/GHSA-wp53-j4wj-2cfg
https://nvd.nist.gov/vuln/detail/CVE-2026-0603	8,3	Hibernate	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')		https://access.redhat.com/security/cve/CVE-2026-0603 https://bugzilla.redhat.com/show_bug.cgi?id=2427147
https://nvd.nist.gov/vuln/detail/CVE-2026-24400	8,2	AssertJ	Improper Restriction of XML External Entity Reference	Starting in version 1.4.0 and prior to version 3.27.7	https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html https://github.com/assertj/assertj/commit/85ca7eb6609bb179c043b85ae7d290523b1ba79a https://github.com/assertj/assertj/releases/tag/assertj-build-3.27.7 https://github.com/assertj/assertj/security/advisories/GHSA-rqfh-9r24-8c9r

https://nvd.nist.gov/vuln/detail/CVE-2026-24470	8,1	Skipper	Unintended Proxy or Intermediary ('Confused Deputy')	Prior to version 0.24.0	https://github.com/zalando/skipper/commit/a4c87ce029a58eb8e1c2c1f93049194a39cf6219 https://github.com/zalando/skipper/security/advisories/GHSA-mxxc-p822-2hx9 https://kubernetes.io/docs/concepts/services-networking/service/#externalname
https://nvd.nist.gov/vuln/detail/CVE-2021-47896	7,8	PDF Complete	Unquoted Search Path or Element	PDF Complete Corporate Edition 4.1.45	https://pdf-complete.informer.com/download/ https://www.exploit-db.com/exploits/49558 https://www.pdfcomplete.com/cms/dpl/tabid/111/Default.aspx?r=du2vH8r https://www.vulncheck.com/advisories/pdfcomplete-corporate-edition-pdfcdispatcher-unquoted-service-path
https://nvd.nist.gov/vuln/detail/CVE-2021-47898	7,8	Epson	Unquoted Search Path or Element	Epson USB Display 1.6.0.0	https://epson.com.mx/ https://www.exploit-db.com/exploits/49548 https://www.vulncheck.com/advisories/epson-usb-display-unquoted-service-path-vulnerability
https://nvd.nist.gov/vuln/detail/CVE-2025-67264	7,8	Doogee	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Doogee Note59, Note59 Pro, and Note59 Pro+	http://doogee.com https://github.com/Skorpion96/unisoc-su/blob/main/CVE-2025-67264.md
https://nvd.nist.gov/vuln/detail/CVE-2026-21509	7,8	Microsoft Office	Reliance on Untrusted Inputs in a Security Decision		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509 https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-21509
https://nvd.nist.gov/vuln/detail/CVE-2026-22271	7,5	Dell ECS	Cleartext Transmission of Sensitive Information	Dell ECS, versions 3.8.1.0 through 3.8.1.7, and Dell ObjectScale versions prior to 4.2.0.0	https://www.dell.com/support/kbdoc/en-us/000415880/dsa-2026-047-security-update-for-dell-ecs-and-objectscale-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2026-23864	7,5	React Server Components	Uncontrolled Resource Consumption		https://www.facebook.com/security/advisories/cve-2026-23864
https://nvd.nist.gov/vuln/detail/CVE-2026-24469	7,5	C++ HTTP Server	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Versions 1.0 and below	https://github.com/frustratedProton/http-server/security/advisories/GHSA-qp54-6gfq-3gff
https://nvd.nist.gov/vuln/detail/CVE-2026-24536	7,5	webpushr	Exposure of Sensitive System Information to an Unauthorized Control Sphere	from n/a through <= 4.38.0	https://patchstack.com/database/Wordpress/Plugin/webpushr-web-push-notifications/vulnerability/wordpress-webpushr-plugin-4-38-0-sensitive-data-exposure-vulnerability?_s_id=cve

https://nvd.nist.gov/vuln/detail/CVE-2026-24609	7,5	PHP Remote File Inclusion	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusio	from n/a through <= 3.1	https://patchstack.com/database/Wordpress/Theme/laurent/vulnerability/wordpress-laurent-theme-3-1-local-file-inclusion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-27821	7,3	Apache Hadoop HDFS	Out-of-bounds Write	from 3.2.0 before 3.4.2	http://www.openwall.com/lists/oss-security/2026/01/23/7 https://lists.apache.org/thread/kwjhyyx0wl2z9b0mw0styjk0hhdbyplh
https://nvd.nist.gov/vuln/detail/CVE-2026-1412	7,3	Sangfor Operation and Maintenance Security Management System	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	up to 3.0.12	https://github.com/LX-LX88/cve/issues/22 https://vuldb.com/?ctiid.342801 https://vuldb.com/?id.342801 https://vuldb.com/?submit.736513
https://nvd.nist.gov/vuln/detail/CVE-2026-1448	7,3	D-Link	Improper Neutralization of Special Elements used in a Command ('Command Injection')	D-Link DIR-615 up to 4.10	https://pentagonal-time-3a7.notion.site/DIR-615-v4-10-2e7e5dd4c5a580a5aac5c8ce35933396?pvs=73 https://vuldb.com/?ctiid.342880 https://vuldb.com/?id.342880 https://vuldb.com/?submit.737006 https://www.dlink.com/

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 Five Known Exploited Vulnerabilities to Catalog	▪ CVE-2018-14634 Linux Kernel Integer Overflow Vulnerability ▪ CVE-2025-52691 SmarterTools SmarterMail Unrestricted Upload of File with Dangerous Type Vulnerability ▪ CVE-2026-21509 Microsoft Office Security Feature Bypass Vulnerability ▪ CVE-2026-23760 SmarterTools SmarterMail Authentication Bypass Using an Alternate Path or Channel Vulnerability ▪ CVE-2026-24061 GNU InetUtils Argument Injection Vulnerability	https://www.cisa.gov/news-events/alerts/2026/01/26/cisa-adds-five-known-exploited-vulnerabilities-catalog
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2024-37079 Broadcom VMware vCenter Server Out-of-bounds Write Vulnerability	https://www.cisa.gov/news-events/alerts/2026/01/23/cisa-adds-one-known-exploited-vulnerability-catalog
Product Categories for Technologies That Use Post-Quantum Cryptography Standards		https://www.cisa.gov/resources-tools/resources/product-categories-technologies-use-post-quantum-cryptography-standards
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
Microsoft Shares BitLocker Keys with FBI to Unlock Encrypted Laptops in Guam Fraud Investigation	https://cybersecuritynews.com/microsoft-shares-bitlocker-keys/
New Windows Notepad and Paint Update Brings More Useful AI Features	https://cybersecuritynews.com/windows-notepad-and-paint-update-ai-features/
New Windows 11 KB5074109 Update Breaks Systems – Microsoft Asks Users to Remove Update	https://cybersecuritynews.com/windows-11-update-breaks-systems/
ZAP Releases OWASP PenTest Kit Browser Extension for Application Security Testing	https://cybersecuritynews.com/zap-owasp-pentest-kit/
Curl to End Bug Bounty Following Low-Quality AI-Generated Vulnerability Reports	https://cybersecuritynews.com/curl-end-bug-bounty/
MITRE Releases New Cybersecurity Framework to Protect the Embedded Systems	https://cybersecuritynews.com/mitre-releases-framework-protect-embedded-systems/
Microsoft Releases Out-of-Band Update KB5078127 to Fix Windows 11 File System and Outlook Freezes	https://cybersecuritynews.com/microsoft-out-of-band-update-windows-11/
48M Gmail, 6.5M Instagram Exposed Online From Unprotected Database	https://cybersecuritynews.com/48m-gmail-6-5m-instagram-exposed-online/
Microsoft Investigating Boot Failure Issues With Windows 11, version 25H2 Following January Update	https://cybersecuritynews.com/microsoft-investigating-boot-failure/
Hackers Use ‘rn’ Typo Trick to Impersonate Microsoft and Marriott in New Phishing Attack	https://cybersecuritynews.com/rn-typo-phishing-attack/
Microsoft Launches Open-Source WinApp CLI to Streamline Windows App Development	https://cybersecuritynews.com/winapp-cli/

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
Nova Ransomware Allegedly Claiming Breach of KPMG Netherlands	https://cybersecuritynews.com/nova-ransomware-breach-kpmg-netherlands/

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
Microsoft Office Zero-day Vulnerability Actively Exploited in Attacks	https://cybersecuritynews.com/microsoft-office-zero-day-vulnerability-2/
Hundreds of Exposed Clawdbot Gateways Leave API Keys and Private Chats Vulnerable	https://cybersecuritynews.com/clawdbot-chats-exposed/
800K+ Telnet Servers Exposed to RCE Attacks – PoC Released	https://cybersecuritynews.com/800k-gnu-inetutils-telnetd-instances-exposed/
Apache Hadoop Vulnerability Exposes Systems Potential Crashes or Data Corruption	https://cybersecuritynews.com/apache-hadoop-vulnerability/
New Instagram Vulnerability Exposes Private Posts to Anyone	https://cybersecuritynews.com/instagram-vulnerability-private-posts/
CISA Warns of Critical VMware vCenter RCE Vulnerability Exploited in Attacks	https://cybersecuritynews.com/vmware-vcenter-rce-vulnerability/
Hackers Exploiting telnetd Vulnerability for Root Access – Public PoC Released	https://cybersecuritynews.com/telnetd-vulnerability-exploited/
Node.js Updated HackerOne Program to Require a Signal of 1.0 or Higher to Submit Vulnerability Reports	https://cybersecuritynews.com/node-js-updated-hackerone-program/
76 Zero-day Vulnerabilities Uncovered by Hackers on Pwn2Own Automotive 2026	https://cybersecuritynews.com/0-day-vulnerabilities-pwn2own-automotive-2026-2/
Fortinet Confirms Active Exploitation of FortiCloud SSO Authentication Bypass Vulnerability	https://cybersecuritynews.com/fortinet-confirms-active-exploitation/
TrustAsia Revoked 143 Certificates Following LiteSSL ACME Service Vulnerability	https://cybersecuritynews.com/trustasia-revoked-143-certificates/
HPE Alletra and Nimble Storage Vulnerability Grants Admin Access to Remote Attacker	https://cybersecuritynews.com/hpe-alletra-and-nimble-storage-vulnerability/

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
China-Aligned APTs Use PeckBirdy C&C Framework in Multi-Vector Attacks, Exploiting Stolen Certificates	https://cybersecuritynews.com/china-aligned-apts-use-peckbirdy-cc-framework/
Threat Actors Using Fake Notepad++ and 7-zip Websites to Deploy Remote Monitoring Tools	https://cybersecuritynews.com/threat-actors-using-fake-notepad-and-7-zip-websites/
New Malware Toolkit Sends Users to Malicious Websites While the URL Stays the Same	https://cybersecuritynews.com/new-malware-toolkit-sends-users/
Lazarus Hackers Actively Attacking European Drone Manufacturing Companies	https://cybersecuritynews.com/lazarus-hackers-actively-attacking-european-drone/
New DPRK Interview Campaign Leverages Fake Fonts to Deploy Malware	https://cybersecuritynews.com/new-dprk-interview-campaign-leverages-fake-fonts/
'SyncFuture' Campaign Weaponizing Legitimate Enterprise Security Software to Deploy Malware	https://cybersecuritynews.com/syncfuture-campaign-weaponizing-security-software/
New Phishing Attack Leverages Vercel Hosting Platform to Deliver a Remote Access Tool	https://cybersecuritynews.com/new-phishing-attack-leverages-vercel-hosting-platform/
Sandworm APT Group Targeting Poland's Power Grid with DynoWiper Malware	https://cybersecuritynews.com/sandworm-apt-group-targeting-polands-power-grid/
Attackers Targeting Construction Firms Exploiting Mjobtime App Vulnerability Using MSSQL and IIS POST Request	https://cybersecuritynews.com/attackers-exploiting-mjobtime-app-vulnerability/
Threat Actors Fake BSODs and Trusted Build Tools to Bypass Defenses and Deploy DCRat	https://cybersecuritynews.com/threat-actors-fake-bsods-and-trusted-build-tools/
20,000 WordPress Sites Affected by Backdoor Vulnerability Allowing Malicious Admin User Creation	https://cybersecuritynews.com/20000-wordpress-sites-affected-by-backdoor-vulnerability/
Threat Actors Weaponizes LNK File to Deploy MoonPeak Malware Attacking Windows Systems	https://cybersecuritynews.com/threat-actors-weaponizes-lnk-file/
Fake Captcha Ecosystem Exploits Trusted Web Infrastructure to Deliver Malware	https://cybersecuritynews.com/fake-captcha-ecosystem-exploits-trusted-web-infrastructure/
MacSync macOS Infostealer Leverage ClickFix-style Attack to Trick Users Pasting a Single Terminal Command	https://cybersecuritynews.com/macsync-macos-infostealer-leverage-clickfix-style-attack/
Hackers Can Use GenAI to Change Loaded Clean Page Into Malicious within Seconds	https://cybersecuritynews.com/hackers-can-use-genai-to-change-loaded-clean-page/
New Phishing Kit As-a-service Attacking Google, Microsoft, and Okta Users	https://cybersecuritynews.com/new-phishing-kit-as-a-service-attacking/
New Watering Hole Attacking EmEditor User with Stealer Malware	https://cybersecuritynews.com/new-watering-hole-attacking-emeditor-users/
North Korean Hackers Adopted AI to Generate Malware Attacking Developers and Engineering Teams	https://cybersecuritynews.com/north-korean-hackers-adopted-ai-to-generate-malware/
New Lawsuit Claims that Meta Can Read All the WhatsApp Users Messages	https://cybersecuritynews.com/whatsapp-lawsuit/
Threat Actors Leverage SharePoint Services in Sophisticated AiTM Phishing Campaign	https://cybersecuritynews.com/sharepoint-services-in-sophisticated-aitm-phishing-campaign/

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/