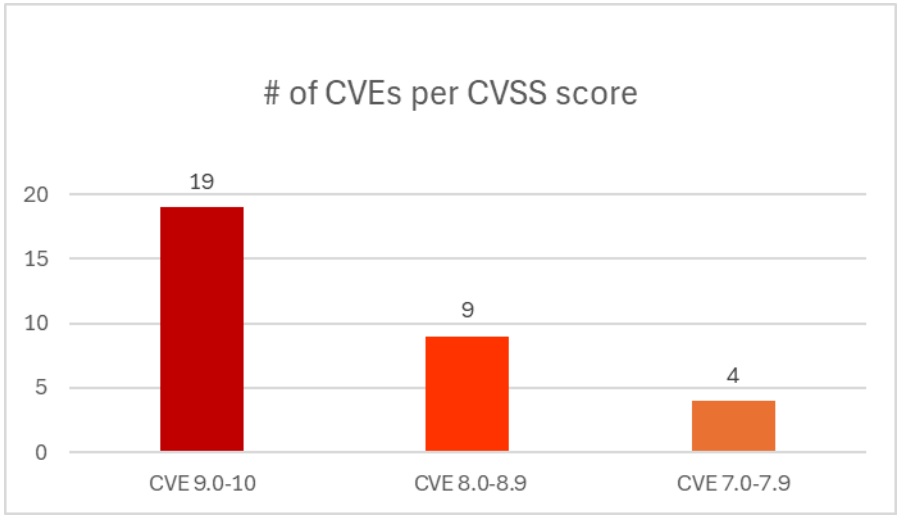
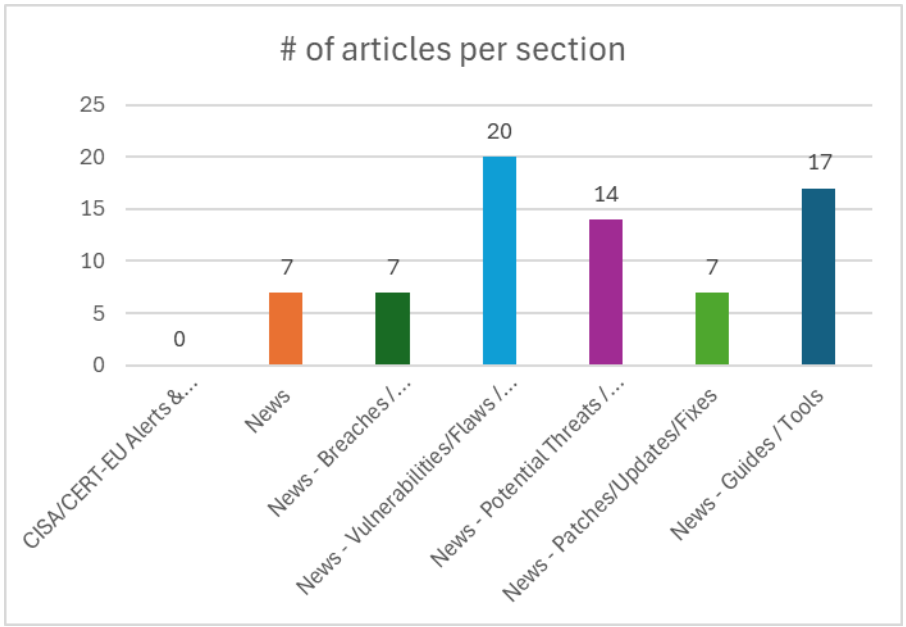


Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 11/11/2026 - 13/11/2026





Contents

Common Vulnerabilities and Exposures (CVEs) 3
CISA/CERT-EU Alerts & Advisories 6
News 7
Breaches / Compromised / Hacked 7
Vulnerabilities / Flaws / Zero-day 8
Patches / Updates / Fixes 10
Potential threats / Threat intelligence 10
Guides / Tools 11
References 13
Annex – Websites with vendor specific vulnerabilities 14

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 όπως 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-2026-126147	9,8	Fortinet FortiMail	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2	https://fortiguard.fortinet.com/psirt/FG-IR-26-199
https://nvd.nist.gov/vuln/detail/cve-2026-126148	9,8	Fortinet FortiMail	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6	https://fortiguard.fortinet.com/psirt/FG-IR-26-200
https://nvd.nist.gov/vuln/detail/cve-2026-126170	9,8	Fortinet FortiAnalyzer	Improper Encoding or Escaping of Output	Fortinet FortiAnalyzer 8.0.0 through 8.0.2, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer Cloud 8.0.1 through 8.0.2, FortiAnalyzer Cloud 7.6.0 through 7.6.7, FortiAnalyzer-BigData 7.6.0 through 7.6.2, FortiManager 8.0.0 through 8.0.2, FortiManager 7.6.0 through 7.6.7, FortiManager Cloud 8.0.1 through 8.0.2, FortiManager Cloud 7.6.0 through 7.6.7	https://fortiguard.fortinet.com/psirt/FG-IR-26-219
https://nvd.nist.gov/vuln/detail/cve-2026-126259	9,8	Fortinet FortiOS	Missing Authentication for Critical Function	Fortinet FortiOS 8.0.0, FortiOS 7.6.0 through 7.6.7, FortiOS 7.4.0 through 7.4.12, FortiOS 7.2.0 through 7.2.13	https://fortiguard.fortinet.com/psirt/FG-IR-26-273
https://nvd.nist.gov/vuln/detail/cve-2026-126262	9,8	Fortinet FortiAnalyzer	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2.0 through 7.2.12, FortiManager 8.0.0, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12	https://fortiguard.fortinet.com/psirt/FG-IR-26-276
https://nvd.nist.gov/vuln/detail/cve-2026-126263	9,8	Fortinet FortiMail	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.4, FortiMail 7.4.0 through 7.4.6	https://fortiguard.fortinet.com/psirt/FG-IR-26-277

https://nvd.nist.gov/vuln/detail/cve-2026-67449	9,8	Portabase	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Portabase is a database backup and restore tool for PostgreSQL, MySQL, MsSQL, MariaDB, Firebird SQL, SQLite, MongoDB, Redis, Files and Docker Volume. Prior to version 1.21.2	https://github.com/Portabase/portabase/commit/8dcb406790728fbdbf758ec88bf000af79498fc1 https://github.com/Portabase/portabase/pull/355 https://github.com/Portabase/portabase/releases/tag/1.21.2 https://github.com/Portabase/portabase/security/advisories/GHSA-7697-vf3j-253j
https://nvd.nist.gov/vuln/detail/cve-2026-76954	9,8	Synology DiskStation Manager (DSM)	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	ynology DiskStation Manager (DSM) before 7.2.1-69057-13, 7.2.2-72806-10, 7.3.2-86009-5, and 7.4.1-90080-1	https://www.synology.com/en-global/security/advisory/Synology_SA_26_19
https://nvd.nist.gov/vuln/detail/cve-2026-126254	9,6	Fortinet FortiOS	Numeric Truncation Error	Fortinet FortiOS 8.0.0 through 8.0.1, FortiOS 7.6.0 through 7.6.7, FortiOS 7.4.0 through 7.4.12, FortiOS 7.2.0 through 7.2.13	https://fortiguard.fortinet.com/psirt/FG-IR-26-268
https://nvd.nist.gov/vuln/detail/cve-2026-126164	9,4	Fortinet FortiMail	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2	https://fortiguard.fortinet.com/psirt/FG-IR-26-216
https://nvd.nist.gov/vuln/detail/cve-2026-126253	9,3	Fortinet FortiOS	Authentication Bypass by Primary Weakness	Fortinet FortiOS 8.0.0 through 8.0.1, FortiOS 7.6.0 through 7.6.7, FortiOS 7.4.0 through 7.4.12, FortiOS 7.2.0 through 7.2.13	https://fortiguard.fortinet.com/psirt/FG-IR-26-267
https://nvd.nist.gov/vuln/detail/cve-2026-126150	9,1	Fortinet FortiMail	Weak Password Recovery Mechanism for Forgotten Password	Fortinet FortiMail 8.0.0, FortiMail 7.6.0 through 7.6.5, FortiMail 7.4.0 through 7.4.7, FortiMail 7.2.0 through 7.2.9	https://fortiguard.fortinet.com/psirt/FG-IR-26-202
https://nvd.nist.gov/vuln/detail/cve-2026-126155	9,1	Fortinet FortiMail	Incorrect Authorization	Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2	https://fortiguard.fortinet.com/psirt/FG-IR-26-207
https://nvd.nist.gov/vuln/detail/cve-2026-126156	9,1	Fortinet FortiMail	uthorization Bypass Through User-Controlled Key	Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2	https://fortiguard.fortinet.com/psirt/FG-IR-26-208
https://nvd.nist.gov/vuln/detail/cve-2026-126156	9,1	Fortinet FortiMail	Authorization Bypass Through User-Controlled Key	Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2	https://fortiguard.fortinet.com/psirt/FG-IR-26-208
https://nvd.nist.gov/vuln/detail/cve-2026-126157	9,1	Fortinet FortiMail	Improper Authentication	Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2	https://fortiguard.fortinet.com/psirt/FG-IR-26-209
https://nvd.nist.gov/vuln/detail/cve-2026-126229	9,1	Fortinet FortiAnalyzer	Authorization Bypass Through User-Controlled Key	Fortinet FortiAnalyzer 8.0.0 through 8.0.1, FortiAnalyzer 7.6.0 through 7.6.7, FortiAnalyzer 7.4.0 through 7.4.11, FortiAnalyzer 7.2.0 through 7.2.12, FortiAnalyzer 7.0 all versions, FortiAnalyzer Cloud 8.0.1, FortiAnalyzer Cloud 7.6.0	https://fortiguard.fortinet.com/psirt/FG-IR-26-244

				through 7.6.7, FortiAnalyzer Cloud 7.4.1 through 7.4.11, FortiAnalyzer Cloud 7.2.1 through 7.2.12, FortiAnalyzer Cloud 7.0 all versions, FortiManager 8.0.0 through 8.0.1, FortiManager 7.6.0 through 7.6.7, FortiManager 7.4.0 through 7.4.11, FortiManager 7.2.0 through 7.2.12, FortiManager 7.0 all versions, FortiManager Cloud 8.0.1, FortiManager Cloud 7.6.0 through 7.6.7, FortiManager Cloud 7.4.1 through 7.4.11, FortiManager Cloud 7.2.1 through 7.2.12, FortiManager Cloud 7.0	
https://nvd.nist.gov/vuln/detail/cve-2026-126251	9,1	Fortinet FortiAuthenticator	Incorrect Authorization	Fortinet FortiAuthenticator 8.0.0 through 8.0.3, FortiAuthenticator 6.6.0 through 6.6.10	https://fortiguard.fortinet.com/psirt/FG-IR-26-265
https://nvd.nist.gov/vuln/detail/cve-2026-126257	9,0	Fortinet FortiAuthenticator	Use of Hard-coded Password	Fortinet FortiAuthenticator 8.0.0 through 8.0.3, FortiAuthenticator 6.6.0 through 6.6.10	https://fortiguard.fortinet.com/psirt/FG-IR-26-271
https://nvd.nist.gov/vuln/detail/cve-2026-18447	8,8	PostgreSQL SQL-language	Access of Resource Using Incompatible Type ('Type Confusion')	Versions before PostgreSQL 18.7, 17.12, 16.16, 15.20, and 14.25 are affected	https://www.postgresql.org/support/security/CVE-2026-18447/
https://nvd.nist.gov/vuln/detail/cve-2026-6460	8,8	PostgreSQL	Access of Resource Using Incompatible Type ('Type Confusion')	-	https://www.postgresql.org/support/security/CVE-2026-6460/
https://nvd.nist.gov/vuln/detail/cve-2026-74857	8,8	Auth API in Synology DiskStation Manager (DSM)	Missing Critical Step in Authentication	Auth API in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1	https://www.synology.com/en-global/security/advisory/Synology_SA_26_18
https://nvd.nist.gov/vuln/detail/cve-2026-91875	8,7	Dell OpenManage Ansible Modules	Improper Certificate Validation	Dell OpenManage Ansible Modules, versions 9.2.0 through 10.0.3	https://www.dell.com/support/kbdoc/en-in/000515420/dsa-2026-432-security-update-for-dell-ansible-server-vulnerabilities
https://nvd.nist.gov/vuln/detail/cve-2026-85101	8,6	Synology DiskStation Manager (DSM)	Authentication Bypass Using an Alternate Path or Channel	Synology DiskStation Manager (DSM) before 7.2.1-69057-13, 7.2.2-72806-10, 7.3.2-86009-5, and 7.4.1-90080-1	https://www.synology.com/en-global/security/advisory/Synology_SA_26_19
https://nvd.nist.gov/vuln/detail/cve-2026-77882	8,5	Lenovo System Update	Deserialization of Untrusted Data	-	https://support.lenovo.com/us/en/downloads/ds012808 https://support.lenovo.com/us/en/product_security/LEN-232748
https://nvd.nist.gov/vuln/detail/cve-2026-18596	8,1	OTP in Synology DiskStation Manager (DSM)	Authentication Bypass Using an Alternate Path or Channel	OTP in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1	https://www.synology.com/en-global/security/advisory/Synology_SA_26_18

https://nvd.nist.gov/vuln/detail/cve-2026-19048	8,1	Synology DiskStation Manager (DSM)	Improper Link Resolution Before File Access ('Link Following')	Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1	https://www.synology.com/en-global/security/advisory/Synology_SA_26_18
https://nvd.nist.gov/vuln/detail/cve-2026-81584	8,1	Synology DiskStation Manager (DSM)	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1	https://www.synology.com/en-global/security/advisory/Synology_SA_26_18
https://nvd.nist.gov/vuln/detail/cve-2026-91891	7,5	Dell Terraform Provider for PowerStore	Insertion of Sensitive Information into Log File	Insertion of Sensitive Information into Log File	https://www.dell.com/support/kbdoc/en-in/000515434/dsa-2026-433-security-update-for-dell-terraform-provider-for-dell-storage-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/cve-2026-126256	7,4	Fortinet FortiOS	Out-of-bounds Read	Fortinet FortiOS 8.0.0 through 8.0.1, FortiOS 7.6.0 through 7.6.7, FortiOS 7.4.0 through 7.4.12, FortiOS 7.2.0 through 7.2.13	https://fortiguard.fortinet.com/psirt/FG-IR-26-270
https://nvd.nist.gov/vuln/detail/cve-2026-91871	7,4	Dell Ansible Storage for PowerStore	Improper Certificate Validation	Dell Ansible Storage for PowerStore, versions prior to 3.9.0	https://www.dell.com/support/kbdoc/en-au/000515361/dsa-2026-431-security-update-for-dell-ansible-storage-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/cve-2026-75785	7,2	VPN API in Synology DiskStation Manager (DSM)		An improper neutralization of special elements used in an OS command vulnerability in the VPN API in Synology DiskStation Manager (DSM) before 7.3.2-86009-5 and 7.4.1-90080-1	https://www.synology.com/en-global/security/advisory/Synology_SA_26_18

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

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 365 Massive Outage – Fixes Fail as Restored Servers Keep Going Unresponsive	https://cybersecuritynews.com/microsoft-365-massive-outage-fixes-fail-as-restored-servers-keep-going-unresponsive/
Massive Microsoft 365 Outage Impacts Exchange Online, Teams, SharePoint, Copilot, and Defender XDR Users	https://cybersecuritynews.com/massive-microsoft-365-outage/
Europol Takes Down 235 Servers and 257 Domains Linked to Gootloader, CastleRAT, and StealC Malware	https://cybersecuritynews.com/malware-infrastructure-disrupted/
Microsoft Teams Outage Hits Users in North America	https://cybersecuritynews.com/microsoft-teams-outagenorth-america/
Qilin Ransomware Admin Identified as 36-Year-Old Russian Hacker After Cybercrime Probe	https://cybersecuritynews.com/qilin-ransomware-admin-identified/
FATF Traces Over $100 Million in Stolen Funds Through Crypto Wallets Linked to Global Scam Networks	https://cybersecuritynews.com/stolen-funds-through-crypto-wallets/
eMudhra Revokes 8 More Certificate Authorities Following Major SSL Private Key Security Failure	https://cybersecuritynews.com/emudhra-certificate-authority-revocation/

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
Google Chrome Fixes 83 Security Flaws, Including 5 Critical Ones that Could Enable RCE Attacks	https://cybersecuritynews.com/google-chrome-fixes-83-security-flaws/
Apache Patches Critical HTTP/2 Flaw Allowing Remote Code Execution on Web Servers	https://cybersecuritynews.com/apache-patches-critical-http-2-flaw/

Σύντομη περιγραφή / Τίτλος	URL
Node.js Fixes 16 Security Flaws That Could Expose TLS Private Keys and Crash Servers Remotely	https://cybersecuritynews.com/node-js-fixes-16-security-vulnerabilities/
Ubuntu 26.10 Adds New Security Protection to curl, Blocking Revoked SSL Certificates	https://cybersecuritynews.com/ubuntu-26-10-adds-protection-to-curl/
N-able Releases Emergency N-central Hotfix After 33 Vulnerabilities Trigger Worldwide Shutdown	https://cybersecuritynews.com/n-able-n-central-security-vulnerabilities/
Git Fixes 6 Security Vulnerabilities Allowing Hackers to Execute Malicious Code Through Cloned Repositories	https://cybersecuritynews.com/git-fixes-security-vulnerabilities/
Microsoft November 2026 Patch Tuesday Fixes 1,093 Vulnerabilities, Including Outlook Zero-Day	https://cybersecuritynews.com/microsoft-november-2026-patch-tuesday/

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
Hackers Exploit Check Point Firewall Flaws to Gain Root Access and Deploy Wiper Malware on VMware ESXi	https://cybersecuritynews.com/hackers-exploit-check-point-firewall-flaws/
New N-able N-central Zero-Day Exploits Target Patched Servers, Claiming Unauthenticated Root Access	https://cybersecuritynews.com/n-able-n-central-zero-day-exploits/
CISA Confirms Active Exploitation of Outlook User Interaction 0-Day Vulnerability	https://cybersecuritynews.com/active-exploitation-of-outlook-0-day-vulnerability/
Critical Red Hat Quay Vulnerability Allows Unauthenticated Attackers to Hijack Container Registries	https://cybersecuritynews.com/red-hat-quay-vulnerability/
AWS MCP Gateway Security Flaw Allowing Access to Internal Networks and Cloud Credentials	https://cybersecuritynews.com/aws-mcp-gateway-security-flaw/
Lenovo Warns of High-Severity Server Flaw That Restores Default Root Credentials After Reset	https://cybersecuritynews.com/lenovo-server-flaw/
CISA Warns of Google Chromium 0-Day Vulnerability Actively Exploited in Attacks	https://cybersecuritynews.com/google-chromium-0-day-vulnerability-exploited/

Critical MongoDB Flaw Lets Attackers Crash Database Servers With Just Two Ping Requests	https://cybersecuritynews.com/mongodb-database-crash-vulnerability/
Palo Alto PAN-OS RCE Flaw Allows Attackers to Execute Arbitrary Code With Root Privileges	https://cybersecuritynews.com/palo-alto-networks-pan-os-rce-vulnerability/
Microsoft Discovers 59 Linux Kernel Security Bugs Using AI, Including Flaws Hidden for Over 20 Years	https://cybersecuritynews.com/linux-kernel-security-bugs/
Windows SignDrop 0-Day Exploit Lets Attackers Gain SYSTEM Privileges Through CLFS Protection	https://cybersecuritynews.com/windows-signdrop-zero-day-exploit/
Windows BitLocker Vulnerabilities Allow Attackers to Bypass Security Feature	https://cybersecuritynews.com/windows-bitlocker-security-bypass/
Multiple Windows Remote Desktop Flaws Allow Attackers to Execute Code Over Network	https://cybersecuritynews.com/multiple-windows-remote-desktop-vulnerabilities/
Hackers Exploit AhsayCBS Vulnerabilities to Hide Malware in PNG Images and Deploy Stealthy Backdoors	https://cybersecuritynews.com/hackers-exploit-ahsaycbs-vulnerabilities/
Windows Active Directory RCE Vulnerability Allows Attacker to Execute Code Over a Network	https://cybersecuritynews.com/windows-active-directory-rce-vulnerability/
Critical Fortinet2Shell Vulnerability Enables RCE Attacks in FortiClient with FortiPAM Enabled	https://cybersecuritynews.com/fortinet2shell-vulnerability/
Critical Fortinet Flaws Expose FortiManager and FortiAnalyzer to Remote Code Execution Without Login	https://cybersecuritynews.com/critical-fortinet-flaws-patched/
Microsoft Confirms Hackers Are Exploiting Outlook 0-Day to Steal Windows Authentication Hashes	https://cybersecuritynews.com/outlook-0-day-vulnerability/
Hackers Can Exploit SAP PROXYGATE and ICM2SHELL Flaws for Unauthorized Full System Access	https://cybersecuritynews.com/sap-proxygate-and-icm2shell-flaws/
Hackers Exploit Check Point Firewall Flaws to Gain Root Access and Deploy Wiper Malware on VMware ESXi	https://cybersecuritynews.com/hackers-exploit-check-point-firewall-flaws/

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
Google Chrome Fixes 83 Security Flaws, Including 5 Critical Ones that Could Enable RCE Attacks	https://cybersecuritynews.com/google-chrome-fixes-83-security-flaws/
Apache Patches Critical HTTP/2 Flaw Allowing Remote Code Execution on Web Servers	https://cybersecuritynews.com/apache-patches-critical-http-2-flaw/
Node.js Fixes 16 Security Flaws That Could Expose TLS Private Keys and Crash Servers Remotely	https://cybersecuritynews.com/node-js-fixes-16-security-vulnerabilities/
Ubuntu 26.10 Adds New Security Protection to curl, Blocking Revoked SSL Certificates	https://cybersecuritynews.com/ubuntu-26-10-adds-protection-to-curl/
N-able Releases Emergency N-central Hotfix After 33 Vulnerabilities Trigger Worldwide Shutdown	https://cybersecuritynews.com/n-able-n-central-security-vulnerabilities/
Git Fixes 6 Security Vulnerabilities Allowing Hackers to Execute Malicious Code Through Cloned Repositories	https://cybersecuritynews.com/git-fixes-security-vulnerabilities/
Microsoft November 2026 Patch Tuesday Fixes 1,093 Vulnerabilities, Including Outlook Zero-Day	https://cybersecuritynews.com/microsoft-november-2026-patch-tuesday/

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
Beast Ransomware Uses Hidden ‘666’ Control Panel to Encrypt Windows Systems and Network Shares	https://cybersecuritynews.com/beast-ransomware/
ArcticRAT Android Malware Uses Hidden VNC to Control Smartphones While Showing Victims a Black Screen	https://cybersecuritynews.com/arcticrat-android-malware/
Hackers Abuse Cruciferra Malware-as-a-Service to Conceal Infostealers and Remote Access Trojans	https://cybersecuritynews.com/cruciferra-malware-as-a-service/
Hackers Abuse AntiFox AI Pentesting Tool to Deploy Webshells and Access AWS Production Secrets	https://cybersecuritynews.com/hackers-abuse-antifox-ai-pentesting-tool/

Σύντομη περιγραφή / Τίτλος	URL
Hackers Target AI Coding Tools to Steal Credentials as Researchers Uncover 103 AI-Linked Cyber Incidents	https://cybersecuritynews.com/hackers-target-ai-coding-tools/
Microsoft Warns Hackers Are Using GSocket Backdoors to Keep Linux Servers Compromised After Patching	https://cybersecuritynews.com/gsocket-backdoors/
Hackers Abuse Windows Group Policy to Deploy Citrus Ransomware and Disable Microsoft Defender	https://cybersecuritynews.com/hackers-abuse-windows-group-policy/
Hackers Could Abuse Microsoft Entra AI Agents to Hijack Enterprise Accounts Without Stealing Passwords	https://cybersecuritynews.com/hackers-could-abuse-microsoft-entra-ai-agents/
AI Hacking Frameworks Like ARTEX, PentAGI, and Agent Zero Found Running on Internet-Accessible Servers	https://cybersecuritynews.com/ai-hacking-frameworks/
Hackers Could Exploit MCP Server Supply Chain Weaknesses to Steal API Keys and Administrator Credentials	https://cybersecuritynews.com/hackers-could-exploit-mcp-server/
Claude Code AI Discovers Technique to Turn Dormant Model Neurons Into Hidden Malware Triggers	https://cybersecuritynews.com/claude-code-ai/
ClickFix Attacks Evolve to Hide Malware in PNG Images and Hijack Windows Domain Controllers	https://cybersecuritynews.com/clickfix-attacks-evolve/
China-Linked Hackers Use Fake Chrome Certificate Warnings to Infect Victims With Sparrow Backdoor	https://cybersecuritynews.com/fake-chrome-certificate/
New GhostFrame Malware Lets Hackers Hijack VMware ESXi VMs and Steal Windows Credentials	https://cybersecuritynews.com/ghostframe-malware-hijack-vmware-esxi/

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 10 Best Network Vulnerability Scanners in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-network-vulnerability-scanners/
Top 10 Best Web Application Vulnerability Scanners in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-web-app-scanners/
Top 10 Best Vulnerability Scanners in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-vulnerability-scanners/

Σύντομη περιγραφή / Τίτλος	URL
Top 10 Best Vulnerability Management Tools in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-vulnerability-management-tools/
Top 10 Best AI Governance (AI TRiSM) Platforms in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-ai-governance-platforms/
OpenAI Launches Two AI Cybersecurity Tools to Automate Penetration Testing and Vulnerability Remediation	https://cybersecuritynews.com/openai-two-ai-cybersecurity-tools/
When Attackers Move at AI Speed, How Can Your SOC Keep Up?	https://cybersecuritynews.com/when-attackers-move-at-ai-speed-how-can-your-soc-keep-up/
Top 10 Best Cybersecurity Maturity Assessment Tools in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-maturity-assessment-tools/
Top 10 Best GDPR Compliance Software in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-gdpr-compliance-software/
Top 10 Best HIPAA Compliance Software in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-hipaa-compliance-software/
Top 10 Best PCI DSS Compliance Tools in 2026 [Ranked & Scored]	https://cybersecuritynews.com/top-10-best-pci-dss-compliance-tools-in-2026-ranked-scored-best-pci-dss-compliance-tools/
Top 10 Best IT & Cyber Risk Management Tools in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-it-cyber-risk-tools/
Top 10 Best Security Policy Management Tools in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-security-policy-management/
Top 10 Best Audit Management Software in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-audit-management-software/
Top 10 Best Security Ratings Services in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-security-ratings-services/
Top 10 Best Third-Party / Vendor Risk Management (TPRM) Tools in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-tprm-tools/
Top 10 Best Compliance Automation Software (SOC 2 / ISO 27001) in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-compliance-automation/

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 CVSS v3.1 score >= 7.0 και αφορούν το διάστημα 24/10/2026–27/10/2026.

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/