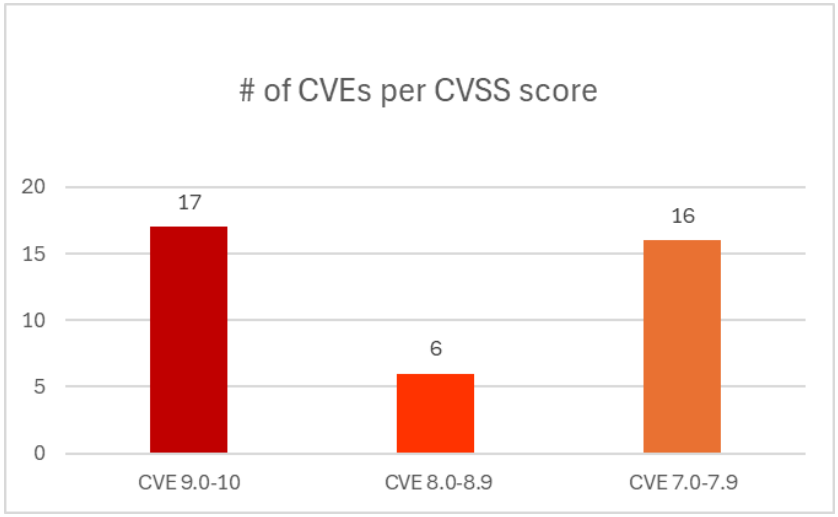
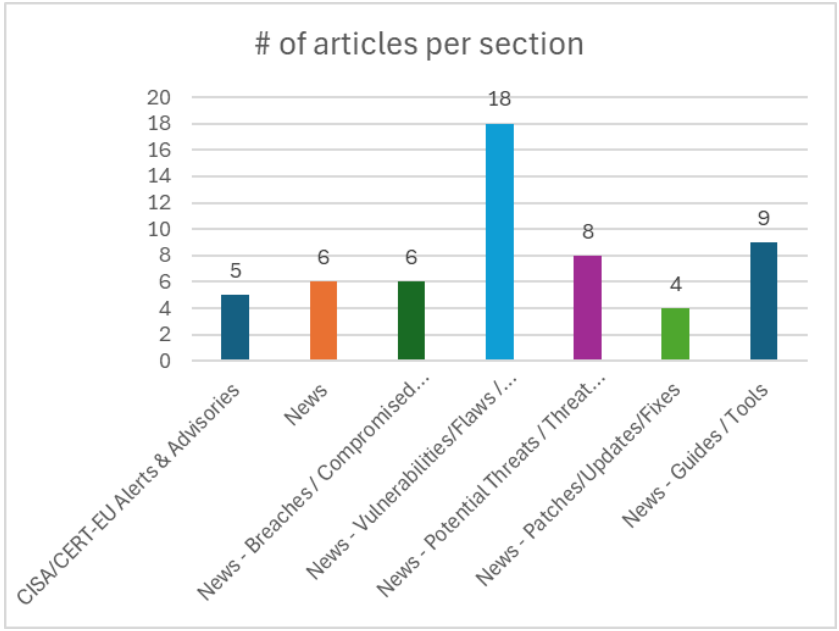
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 04/03/2026 - 06/03/2026





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)	CVSS v3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζο-νται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2026-20131	**10,0**	Cisco Secure Firewall Management Center (FMC)	Deserialization of Untrusted Data		https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh
https://nvd.nist.gov/vuln/detail/CVE-2025-13476	**9,8**	Rakuten Viber Cloak		Rakuten Viber Cloak mode in Android v25.7.2.0g and Windows v25.6.0.0–v25.8.1.0	https://www.kb.cert.org/vuls/id/772695 https://www.viber.com/en/download/
https://nvd.nist.gov/vuln/detail/CVE-2025-29165	**9,8**	D-Link	Improper Privilege Management	D-Link DIR-1253 MESH V1.6.1684	https://codeberg.org/zuhri/advisory/src/branch/main/CVE-2025-29165 https://github.com/twentysevns/Vuln-IoT-Reports/blob/main/DLINK/DIR-1253/README.md https://www.dlink.com/en/security-bulletin/
https://nvd.nist.gov/vuln/detail/CVE-2025-46108	**9,8**	D-link	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	D-link Dir-513 A1FW110	https://github.com/akuma-QAQ/CVEreport/tree/main/D-link/CVE-2025-46108 https://github.com/buobo/bo-s-CVE/blob/main/DIR-513/formTcpipSetup.md https://www.dlink.com/en/security-bulletin/
https://nvd.nist.gov/vuln/detail/CVE-2025-70233	**9,8**	D-Link	Stack-based Buffer Overflow	D-Link DIR-513 v1.10	https://github.com/akuma-QAQ/CVEreport/tree/main/D-link/CVE-2025-70233 https://www.dlink.com.cn/techsupport/ProductInfo.aspx?m=DIR-513 https://www.dlink.com/en/security-bulletin/
https://nvd.nist.gov/vuln/detail/CVE-2026-21536	**9,8**	Microsoft Devices	Unrestricted Upload of File with Dangerous Type	Microsoft Devices Pricing Program Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21536
https://nvd.nist.gov/vuln/detail/CVE-2026-27441	**9,8**	SEPPmail Secure Email Gateway	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	SEPPmail Secure Email Gateway before version 15.0.1	https://downloads.seppmail.com/extrelnotes/150/ERN15.0.html#seppmail-vulnerability-disclosure
https://nvd.nist.gov/vuln/detail/CVE-2026-27647	**9,8**	The WebSocket	Insufficient Session Expiration		https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-057-08.json ICS-CERT Third Party Advisory https://www.cisa.gov/news-events/ics-advisories/icsa-26-057-08 ICS-CERT Third Party Advisory VDB Entry https://www.mobility46.se/en/contact-us

https://nvd.nist.gov/vuln/detail/CVE-2026-27944	9,8	Nginx	Missing Authentication for Critical Function	Prior to version 2.3.3	https://github.com/0xJacky/nginx-ui/security/advisories/GHSA-g9w5-qffc-6762
https://nvd.nist.gov/vuln/detail/CVE-2026-27966	9,8	Langflow	Improper Control of Generation of Code ('Code Injection')	Prior to version 1.8.0	https://github.com/langflow-ai/langflow/commit/d8c6480daa17b2f2af0b5470cdf5c3d28dc9e508 GitHub, Inc. Patch https://github.com/langflow-ai/langflow/security/advisories/GHSA-3645-fxcv-hqr4
https://nvd.nist.gov/vuln/detail/CVE-2026-29058	9,8	AVideo	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Prior to version 7.0	https://github.com/WWBN/AVideo-Encoder/security/advisories/GHSA-9j26-99jh-v26q
https://nvd.nist.gov/vuln/detail/CVE-2026-3000	9,8	IDExpert Windows Logon Agent	Download of Code Without Integrity Check		https://www.changingtec.com/news_detail.jsp?item_id=348 TWCERT/CC https://www.twcert.org.tw/en/cp-139-10741-daed4-2.html TWCERT/CC https://www.twcert.org.tw/tw/cp-132-10740-b2eb2-1.html
https://nvd.nist.gov/vuln/detail/CVE-2026-3422	9,8	U-Office Force	Deserialization of Untrusted Data		https://www.twcert.org.tw/en/cp-139-10743-9a952-2.html TWCERT/CC https://www.twcert.org.tw/tw/cp-132-10742-45b13-1.html
https://nvd.nist.gov/vuln/detail/CVE-2025-69969	9,6	Bluetooth Low Energy (BLE) communication protocol of SRK Powertech Pvt Ltd	Missing Encryption of Sensitive Data	Bluetooth Low Energy (BLE) communication protocol of SRK Powertech Pvt Ltd Pebble Prism Ultra v2.9.2	https://github.com/mukundbhuva/BLEached-Security https://github.com/mukundbhuva/BLEached-Security/security/advisories/GHSA-cp6q-87g8-mq77
https://nvd.nist.gov/vuln/detail/CVE-2026-3545	9,6	Google Chrome	Improper Input Validation	Google Chrome prior to 145.0.7632.159	https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop.html https://issues.chromium.org/issues/487383169
https://nvd.nist.gov/vuln/detail/CVE-2026-22552	9,4	WebSocket	Missing Authentication for Critical Function		https://epower.ie/support/ https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-062-07.json https://www.cisa.gov/news-events/ics-advisories/icsa-26-062-07
https://nvd.nist.gov/vuln/detail/CVE-2026-28484	9,3	OpenClaw	Improper Neutralization of Special Elements used in a Command ('Command Injection')	OpenClaw versions prior to 2026.2.15	https://github.com/openclaw/openclaw/commit/b88f37762f5b6d7ec0f589eb761815e466e4ef4b https://github.com/openclaw/openclaw/commit/ba84b1253967143692166023f9e174c149b6f2ed https://github.com/openclaw/openclaw/security/advisories/GHSA-mmpf-jwf4-h3qv https://www.vulncheck.com/advisories/openclaw-option-injection-in-pre-commit-hook-via-malicious-filenames
https://nvd.nist.gov/vuln/detail/CVE-2026-20764	8,8	XWEB Pro	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	1.12.1 and prior	https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-057-10.json ICS-CERT Third Party Advisory

					https://webapps.copeland.com/Dixell/Pages/SystemSoftwareUpdate ICS-CERT Product https://www.cisa.gov/news-events/ics-advisories/icsa-26-057
https://nvd.nist.gov/vuln/detail/CVE-2026-27969	**8,8**	Vitess	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Prior to versions 23.0.3 and 22.0.4	https://github.com/vitessio/vitess/commit/c565cab615bc962bda061dcd645aa7506c59ca4a GitHub, Inc. Patch https://github.com/vitessio/vitess/pull/19470 GitHub, Inc. Issue Tracking Patch https://github.com/vitessio/vitess/security/advisories/GHSA-r492-hjgh-c9gw
https://nvd.nist.gov/vuln/detail/CVE-2026-28363	**8,8**	OpenClaw	Incomplete List of Disallowed Inputs	before 2026.2.23	https://github.com/openclaw/openclaw/security/advisories/GHSA-3c6h-g97w-fg78
https://nvd.nist.gov/vuln/detail/CVE-2026-3400	**8,8**	Tenda AC15	Stack-based Buffer Overflow	up to 15.13.07.13	https://vuldb.com/?ctiid.348295 VulDB https://vuldb.com/?id.348295 VulDB https://vuldb.com/?submit.760109 VulDB https://www.tenda.com.cn/ VulDB https://www.yuque.com/ba1ma0-an29k/nnxoap/tzg68iadbmqx6esm?singleDoc#
https://nvd.nist.gov/vuln/detail/CVE-2026-20101	**8,6**	SAML 2.0 single sign-on (SSO) feature of Cisco Secure Firewall ASA	Use of Insufficiently Random Values		https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpn-m9sx6MbC
https://nvd.nist.gov/vuln/detail/CVE-2026-28562	**8,2**	wpForo	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	2.4.14	https://wordpress.org/plugins/wpforo/ VulnCheck https://wordpress.org/plugins/wpforo/#developers VulnCheck https://www.vulncheck.com/advisories/wpforo-sql-injection-via-topics-order-by-parameter
https://nvd.nist.gov/vuln/detail/CVE-2026-28364	**7,9**	In Ocaml	Buffer Over-read	before 4.14.3 and 5.x before 5.4.1	https://github.com/ocaml/security-advisories/blob/generated-osv/2026/OSEC-2026-01.json MITRE https://osv.dev/vulnerability/OSEC-2026-01
https://nvd.nist.gov/vuln/detail/CVE-2026-26949	**7,8**	Dell	Incorrect Authorization	Dell Device Management Agent (DDMA), versions prior to 26.02	https://www.dell.com/support/kbdoc/en-us/000429177/dsa-2026-105
https://nvd.nist.gov/vuln/detail/CVE-2026-27750	**7,8**	Avira Internet Security	Time-of-check Time-of-use (TOCTOU) Race Condition		https://blog.quarkslab.com/avira-deserialize-delete-and-escalate-the-proper-way-to-use-an-av.html https://support.avira.com/hc/en-us/articles/360010656158-Current-Avira-versions https://www.avira.com/en/internet-security https://www.vulncheck.com/advisories/avira-internet-security-optimizer-toctou

https://nvd.nist.gov/vuln/detail/CVE-2026-20105	7,7	Cisco Secure Firewall Adaptive Security Appliance (ASA)	Missing Release of Memory after Effective Lifetime		https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpn-m9sx6MbC
https://nvd.nist.gov/vuln/detail/CVE-2025-13673	7,5	The Tutor LMS	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	all versions up to, and including, 3.9.6	https://plugins.trac.wordpress.org/changeset/3469242/tutor Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/007df869-dacb-4b0a-9c98-50586934cdab?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-2428	7,5	The Fluent Forms Pro Add On Pack plugin for WordPress	Insufficient Verification of Data Authenticity	all versions up to, and including, 6.1.17	https://fluentforms.com/docs/changelog/#2-toc-title Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/e5c62e54-da06-4b44-ba70-63065e664b0d?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-2471	7,5	The WP Mail Logging plugin for WordPress	Deserialization of Untrusted Data	up to, and including, 1.15.0	https://plugins.trac.wordpress.org/browser/wp-mail-logging/tags/1.15.0/lib/vendor/brandonwamboldt/wp-orm/src/BaseModel.php#L39 Wordfence https://plugins.trac.wordpress.org/browser/wp-mail-logging/tags/1.15.0/src/Renderer/WPML_MailRenderer_AJAX_Handler.php#L100 Wordfence https://plugins.trac.wordpress.org/browser/wp-mail-logging/tags/1.15.0/src/WPML_Plugin.php#L553 Wordfence https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3464813%40wp-mail-logging&old=3358334%40wp-mail-logging&sfp_email=&sfph_mail= Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/10e4c52d-c82f-4393-9a56-5714b3a108d1?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-25907	7,5	Dell PowerScale OneFS	Overly Restrictive Account Lockout Mechanism	Dell PowerScale OneFS, version 9.13.0.0	https://www.dell.com/support/kbdoc/en-sg/000434591/dsa-2026-095-security-update-for-dell-powerscale-onefs-overly-restrictive-account-lockout-mechanism-vulnerability
https://nvd.nist.gov/vuln/detail/CVE-2026-27449	7,5	Umbraco Engage	Improper Access Control	prior to versions 16.2.1 and 17.1.1	https://github.com/umbraco/Umbraco.Engage.Issues/security/advisories/GHSA-86vq-ccwf-rm62
https://nvd.nist.gov/vuln/detail/CVE-2026-2747	7,5	SEPPmail Secure Email Gateway	Exposure of Sensitive Information to an Unauthorized Actor	SEPPmail Secure Email Gateway before version 15.0.1	https://downloads.seppmail.com/extrelnotes/150/ERN15.0.html#seppmail-vulnerability-disclosure
https://nvd.nist.gov/vuln/detail/CVE-2026-3395	7,3	MaxSite CMS	Improper Control of Generation of Code ('Code Injection')	up to 109.1	https://github.com/maxsite/cms/ VulDB https://github.com/maxsite/cms/commit/08937a3c5d672a242d68f53e9fccf8a748820ef3 VulDB https://vuldb.com/?ctiid.348281 VulDB https://vuldb.com/?id.348281 VulDB https://vuldb.com/?submit.762169

https://nvd.nist.gov/vuln/detail/CVE-2026-3406	**7,3**	Online Art Gallery Shop	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/ubfbuz3/cve/issues/55 VulDB https://vuldb.com/?ctiid.348301 VulDB https://vuldb.com/?id.348301 VulDB https://vuldb.com/?submit.763740
https://nvd.nist.gov/vuln/detail/CVE-2026-3409	**7,3**	eosphoros-ai db-gpt	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	0.7.5	https://gist.github.com/YLChen-007/d2799d8b2077e50658f12a45bcae9b70 VulDB https://vuldb.com/?ctiid.348304 VulDB https://vuldb.com/?id.348304 VulDB https://vuldb.com/?submit.763745
https://nvd.nist.gov/vuln/detail/CVE-2026-3410	**7,3**	Society Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
https://nvd.nist.gov/vuln/detail/CVE-2026-3413	**7,3**	University Management System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/JXBbozaihuang/vuln-research/issues/1 VulDB https://itsourcecode.com/ VulDB https://vuldb.com/?ctiid.348308 VulDB https://vuldb.com/?id.348308 VulDB https://vuldb.com/?submit.764004
https://nvd.nist.gov/vuln/detail/CVE-2026-20062	**7,2**	CLI of Cisco Secure Firewall Adaptive Security Appliance (ASA)	Incorrect Execution-Assigned Permissions		https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-scpcxt-filecpy-rgeP73nE

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-2017-7921 Hikvision Multiple Products Improper Authentication Vulnerability ▪ CVE-2021-22681 Rockwell Multiple Products Insufficient Protected Credentials Vulnerability ▪ CVE-2021-30952 Apple Multiple Products Integer Overflow or Wraparound Vulnerability ▪ CVE-2023-41974 Apple iOS and iPadOS Use-After-Free Vulnerability ▪ CVE-2023-43000 Apple Multiple products Use-After-Free Vulnerability	https://www.cisa.gov/news-events/alerts/2026/03/05/cisa-adds-five-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
VMware Aria Operations Bug Exploited, Cloud Resources at Risk	https://www.darkreading.com/cloud-security/vmware-aria-operations-bug-exploited-cloud-risk
Global Takedown Neutralizes Tycoon2FA Phishing Service	https://www.infosecurity-magazine.com/news/global-takedown-tycoon2fa-phishing/
Europol Operation Seizes LeakBase Data Breach Site	https://www.infosecurity-magazine.com/news/europol-seizes-leakbase-data/
Coalition of Western Countries Launches 6G Cybersecurity Guidelines	https://www.infosecurity-magazine.com/news/gcot-6g-cybersecurity-guidelines/
Operation Leak Dismantles LeakBase Cybercriminal Forum – User Data, IP Logs Secured by Authorities	https://cybersecuritynews.com/operation-leak-dismantles-leakbase/
Escalating Iranian APT Threats Against Critical Infrastructure Amid Geopolitical Conflict	https://cybersecuritynews.com/escalating-iranian-apt-threats-against-critical-infrastructure/

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**
San Francisco Children's Council warns 12,000+ people of data breach that leaked SSNs	https://www.comparitech.com/news/san-francisco-childrens-council-warns-12000-people-of-data-breach-that-leaked-ssns/?&web_view=true
Hacker mass-mails HungerRush extortion emails to restaurant patrons	https://www.bleepingcomputer.com/news/security/hacker-mass-mails-hungerrush-extortion-emails-to-restaurant-patrons/?&web_view=true
LexisNexis confirms data breach as hackers leak stolen files	https://www.bleepingcomputer.com/news/security/lexisnexis-confirms-data-breach-as-hackers-leak-stolen-files/?&web_view=true
AWS Middle East (UAE) Region Hit by Drone Strikes, 109 Services Disrupted	https://cybersecuritynews.com/aws-middle-east-services-disrupted/
Perplexity's Comet Browser Hijacked Using Calendar Invite to Exfiltrate Sensitive Data	https://cybersecuritynews.com/perplexitys-comet-browser-hijacked/
Coruna Exploit Kit With 23 Exploits Hacked Thousands of iPhones	https://cybersecuritynews.com/coruna-ios-exploit-kit/

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
Hikvision and Rockwell Automation CVSS 9.8 Flaws Added to CISA KEV Catalog	https://thehackernews.com/2026/03/hikvision-and-rockwell-automation-cvss.html
Cisco Confirms Active Exploitation of Two Catalyst SD-WAN Manager Vulnerabilities	https://thehackernews.com/2026/03/cisco-confirms-active-exploitation-of.html
CISA Adds Actively Exploited VMware Aria Operations Flaw CVE-2026-22719 to KEV Catalog	https://thehackernews.com/2026/03/cisa-adds-actively-exploited-vmware.html
Google Confirms 90 Zero-Day Vulnerabilities Actively Exploited in 2025	https://cybersecuritynews.com/google-confirms-90-zero-day-vulnerabilities-exploit-in-2025/
PoC Exploit Released Cisco SD-WAN 0-Day Vulnerability Exploited in the Wild	https://cybersecuritynews.com/poc-exploit-cisco-sd-wan-0-day-vulnerability/
ContextCrush Flaw Exposes AI Development Tools to Attacks	https://www.infosecurity-magazine.com/news/contextcrush-ai-development-tools/
Cisco Drops 48 New Firewall Vulnerabilities, 2 Critical	https://www.darkreading.com/vulnerabilities-threats/cisco-48-firewall-vulnerabilities-2-critical
Critical FreeScout Vulnerability Leads to Full Server Compromise	https://www.securityweek.com/critical-freescout-vulnerability-leads-to-full-server-compromise/
Google: Half of 2025's 90 Exploited Zero-Days Aimed at Enterprises	https://www.securityweek.com/google-half-of-2025s-90-exploited-zero-days-aimed-at-enterprises/
WordPress membership plugin bug exploited to create admin accounts	https://www.bleepingcomputer.com/news/security/wordpress-membership-plugin-bug-exploited-to-create-admin-accounts/
Mail2Shell zero-click attack lets hackers hijack FreeScout mail servers	https://www.bleepingcomputer.com/news/security/mail2shell-zero-click-attack-lets-hackers-hijack-freescout-mail-servers/
Cisco Secure Firewall Management Vulnerability Allow Attackers to Bypass Authentication	https://cybersecuritynews.com/cisco-secure-firewall-management-vulnerability-allow-attackers-to-bypass-authentication/
New MongoDB Vulnerability Lets Hackers Crash Any MongoDB Server	https://cybersecuritynews.com/mongodb-vulnerability-crash-server/
CISA warns of Qualcomm Chipsets Memory Corruption Vulnerability Exploited in Attacks	https://cybersecuritynews.com/qualcomm-chipsets-memory-corruption-vulnerability/
IPVanish VPN for macOS Vulnerability Let Attackers Escalate Privilege and Execute Arbitrary Code	https://cybersecuritynews.com/ipvanish-vpn-for-macos-vulnerability/
Critical XSS Vulnerability in Angular i18n Enables Malicious Code Execution	https://cybersecuritynews.com/xss-vulnerability-in-angular-i18n/
HPE AutoPass Vulnerability Let Attackers Bypass Authentication Remotely	https://cybersecuritynews.com/hpe-autopass-vulnerability/
MS-Agent Vulnerability Let Attackers Hijack AI Agent to Gain Full System Control	https://cybersecuritynews.com/ms-agent-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
OpenAI Launches GPT-5.4 With Advanced Reasoning, Coding, and Computer-Use Capabilities	https://cybersecuritynews.com/gpt-5-4-launched/
Cisco Issues Patches for 48 Vulnerabilities in Enterprise Networking Products	https://www.infosecurity-magazine.com/news/cisco-issues-patches-48/
Google Releases Emergency Chrome Update to Fix 10 Security Vulnerabilities	https://cybersecuritynews.com/critical-chrome-emergency-update/
Windows 10 Update KB5068164 Breaks Windows Recovery Environment	https://cybersecuritynews.com/windows-10-update-kb5068164/

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
ThreatsDay Bulletin: DDR5 Bot Scalping, Samsung TV Tracking, Reddit Privacy Fine & More	https://thehackernews.com/2026/03/threatsday-bulletin-redis-rce-ddr5-bot.html
Hackers Can Use Indirect Prompt Injection Allows Adversaries to Manipulate AI Agents with Content	https://cybersecuritynews.com/hackers-can-use-indirect-prompt-injection-allows-adversaries/
Calls for Global Digital Estate Standard as Posthumous Deepfake Fraud Risk Grows	https://www.infosecurity-magazine.com/news/digital-estate-post-death-deepfake/
Threat Actors Using Fake Claude Code Download to Deploy Infostealer	https://cybersecuritynews.com/threat-actors-using-fake-claude-code/
Surge in Attacks on Surveillance Cameras Linked to Iranian Hackers	https://www.infosecurity-magazine.com/news/iran-attacks-surveillance-cameras/
Hackers Mimic LastPass Support Email to Steal Vault Passwords	https://cybersecuritynews.com/hackers-mimic-lastpass-support-email/
VoidLink Malware Framework Attacking Kubernetes and AI Workloads	https://cybersecuritynews.com/voidlink-malware-framework/
Trusted Azure Utility AzCopy Turned into Data Exfiltration Tool in Active Ransomware Campaigns	https://cybersecuritynews.com/trusted-azure-utility-azcopy-turned/

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/
Splunk Releases Guide to Detect Remote Employment Fraud Within Your Organization	https://cybersecuritynews.com/detect-remote-employment-fraud/
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/
Top 10 Best Exposure Management Tools In 2026	https://cybersecuritynews.com/best-exposure-management-tools/
NETREAPER Offensive Security Toolkit That Wraps 70+ Penetration Testing Tools	https://cybersecuritynews.com/netreaper-offensive-security-toolkit/
GitLab Security Best Practices Cheat Sheet	https://thehackernews.uk/gitlab-security-tips
False Negatives Are a New SOC Headache. Here’s the Fast Way to Fix It	https://cybersecuritynews.com/false-negatives-are-a-new-soc-headache-heres-the-fast-way-to-fix-it/
PentAGI – Automated AI-Powered Penetration Testing Tool that Integrates 20+ Security Tools	https://cybersecuritynews.com/pentagi-penetration-testing-tool/

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/