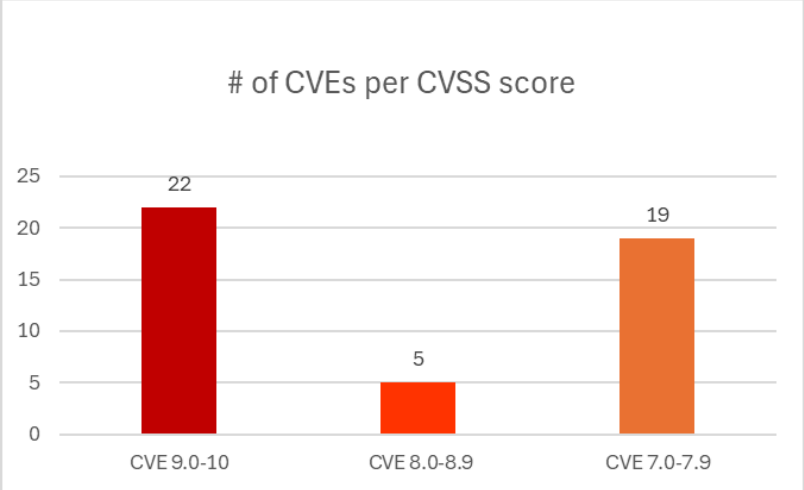
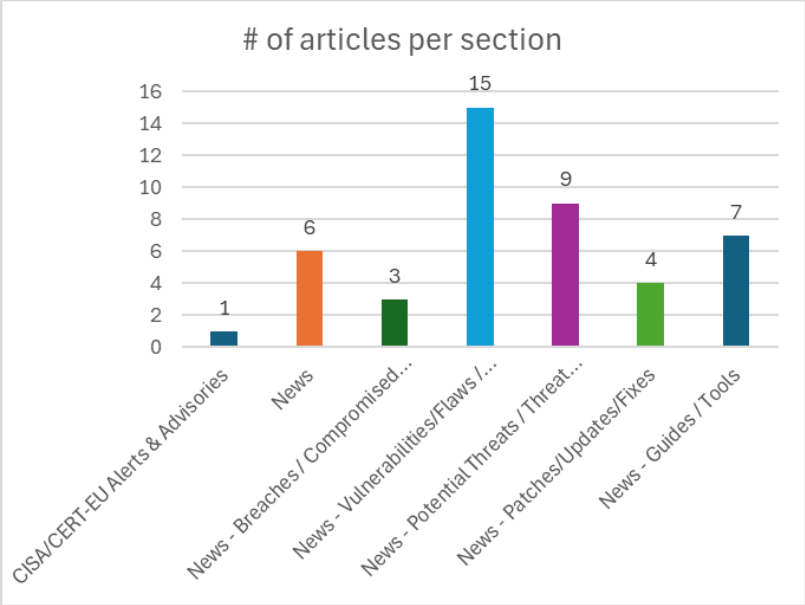
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 04/07/2026 - 07/07/2026





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-2026-57572	10,0	Crawl4AI	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	Crawl4AI Prior to 0.9.0	https://github.com/unclecode/crawl4ai/commit/60886d1a0c52682e4c83a7cef9dfac417fff6bd2 https://github.com/unclecode/crawl4ai/security/advisories/GHSA-r253-r9jw-qg44
https://nvd.nist.gov/vuln/detail/CVE-2026-34037	9,9	Coolify	Authorization Bypass Through User-Controlled Key	Coolify Prior to 4.0.0-beta.464	https://github.com/coollabsio/coolify/commit/1759a1631cd63271ebf6caa250c6d93440eaa333 https://github.com/coollabsio/coolify/releases/tag/v4.0.0-beta.464 https://github.com/coollabsio/coolify/security/advisories/GHSA-ggrr-wrvr-x83v
https://nvd.nist.gov/vuln/detail/CVE-2026-34038	9,9	Coolify	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Coolify Prior to 4.0.0-beta.469	https://github.com/coollabsio/coolify/commit/23f9156c7306b221101f1ebbe4d3c6b5e2522acd https://github.com/coollabsio/coolify/pull/9007 https://github.com/coollabsio/coolify/releases/tag/v4.0.0-beta.469 https://github.com/coollabsio/coolify/security/advisories/GHSA-qqrq-r9h4-x6wp
https://nvd.nist.gov/vuln/detail/CVE-2026-34047	9,9	Coolify	Incorrect Authorization	Coolify Prior to 4.0.0-beta.471	https://github.com/coollabsio/coolify/commit/bc91b41f92f1bbb53886a5d7a60335cbf1621cd5 https://github.com/coollabsio/coolify/pull/9169 https://github.com/coollabsio/coolify/releases/tag/v4.0.0-beta.471 https://github.com/coollabsio/coolify/security/advisories/GHSA-652w-qv22-2r7c
https://nvd.nist.gov/vuln/detail/CVE-2026-34048	9,9	Coolify	Improper Authorization	Coolify Prior to 4.0.0-beta.471	https://github.com/coollabsio/coolify/commit/847166a3f89b7c80972fa0d2e5c754976f95b6ad https://github.com/coollabsio/coolify/releases/tag/v4.0.0-beta.471 https://github.com/coollabsio/coolify/security/advisories/GHSA-mw6q-2hmg-mhxv
https://nvd.nist.gov/vuln/detail/CVE-2026-48614	9,9	Plesk XML API	Improper Control of Generation of Code ('Code Injection')	Plesk XML API	https://support.plesk.com/hc/en-us/articles/41171817973143-Vulnerability-in-Plesk-XML-API
https://nvd.nist.gov/vuln/detail/CVE-2026-14807	9,8	ERP App	Use of Hard-coded Credentials	ERP App	https://www.twcert.org.tw/en/cp-139-11024-c5c1a-2.html https://www.twcert.org.tw/tw/cp-132-11023-3abe8-1.html
https://nvd.nist.gov/vuln/detail/CVE-2026-14808	9,8	Prog Management System	Exposure of Sensitive System Information to an Unauthorized Control Sphere	Prog Management System	https://www.twcert.org.tw/en/cp-139-11026-3df18-2.html https://www.twcert.org.tw/tw/cp-132-11025-fa1d9-1.html
https://nvd.nist.gov/vuln/detail/CVE-2026-24014	9,8	Apache IoTDB	Improper Access Control	Apache IoTDB: from 1.3.3 before 2.0.8	http://www.openwall.com/lists/oss-security/2026/07/06/12 https://lists.apache.org/thread/38298f803gb5j9nlhf0l9zkf34o90h3m

https://nvd.nist.gov/vuln/detail/CVE-2026-43867	9,8	Apache Camel	Deserialization of Untrusted Data	Apache Camel: from 4.18.0 before 4.18.3, from 4.19.0 before 4.21.0	https://camel.apache.org/security/CVE-2026-43867.html
https://nvd.nist.gov/vuln/detail/CVE-2026-46454	9,8	Apache Camel	Improper Input Validation	Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0	http://www.openwall.com/lists/oss-security/2026/07/05/7 https://camel.apache.org/security/CVE-2026-46454.html
https://nvd.nist.gov/vuln/detail/CVE-2026-46455	9,8	Apache Camel	Insufficient Session Expiration	Apache Camel: from 4.18.0 before 4.18.3, from 4.19.0 before 4.21.0	http://www.openwall.com/lists/oss-security/2026/07/05/8 https://camel.apache.org/security/CVE-2026-46455.html
https://nvd.nist.gov/vuln/detail/CVE-2026-46456	9,8	Apache Camel	Improper Input Validation	Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0	http://www.openwall.com/lists/oss-security/2026/07/05/9 https://camel.apache.org/security/CVE-2026-46456.html
https://nvd.nist.gov/vuln/detail/CVE-2026-48204	9,8	Apache Camel	Improper Input Validation	Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0	http://www.openwall.com/lists/oss-security/2026/07/05/18 https://camel.apache.org/security/CVE-2026-48204.html
https://nvd.nist.gov/vuln/detail/CVE-2026-56140	9,8	Apache Camel	Improper Input Validation	Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0	https://camel.apache.org/security/CVE-2026-56140.html
https://nvd.nist.gov/vuln/detail/CVE-2026-9181	9,8	ArcGIS Server	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	ArcGIS Server 12.0 and prior	https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/may-2026-arcgis-security-bulletin
https://nvd.nist.gov/vuln/detail/CVE-2026-57571	9,6	Crawl4AI	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Crawl4AI Prior to 0.9.1	https://github.com/unclecode/crawl4ai/commit/60886d1a0c52682e4c83a7cef9dfac417fff6bd2 https://github.com/unclecode/crawl4ai/security/advisories/GHSA-2jq4-q6vv-4cp3
https://nvd.nist.gov/vuln/detail/CVE-2026-24013	9,1	Apache IoTDB	Authentication Bypass by Spoofing	Apache IoTDB: from 1.3.3 before 2.0.8	http://www.openwall.com/lists/oss-security/2026/07/06/11 https://lists.apache.org/thread/6pwkgnqhbm56mvn309f87snm84s0b75y
https://nvd.nist.gov/vuln/detail/CVE-2026-40047	9,1	Apache Camel	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	Apache Camel: from 4.15.0 before 4.18.3	http://www.openwall.com/lists/oss-security/2026/07/05/2 https://camel.apache.org/security/CVE-2026-40047.html
https://nvd.nist.gov/vuln/detail/CVE-2026-48203	9,1	Apache Camel	Improper Input Validation	Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0	http://camel.apache.org/security/CVE-2026-48203.html http://www.openwall.com/lists/oss-security/2026/07/05/17
https://nvd.nist.gov/vuln/detail/CVE-2026-48205	9,1	Apache Camel	Improper Input Validation	Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0	http://www.openwall.com/lists/oss-security/2026/07/05/19 https://camel.apache.org/security/CVE-2026-48205.html
https://nvd.nist.gov/vuln/detail/CVE-2026-5268	9,1	Ciena	Authentication Bypass Using an Alternate Path or Channel	Ciena	https://www.ciena.com/product-security

https://nvd.nist.gov/vuln/detail/CVE-2026-34158	8,8	Coolify	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Coolify Prior to 4.0.0-beta.469	https://github.com/coollabsio/coolify/security/advisories/GHSA-j6j2-frv3-g6f7
https://nvd.nist.gov/vuln/detail/CVE-2026-9085	8,8	Pardus-Parental-Control	Improper Access Control	Pardus-Parental-Control: from <=0.5.1 before 0.7.0	https://siberguvenlik.gov.tr/guvenlik-bildirimleri/detay/tr-26-0500
https://nvd.nist.gov/vuln/detail/CVE-2025-53828	8,5	SharePoint for ownCloud	Server-Side Request Forgery (SSRF)	SharePoint for ownCloud prior to version 0.4.1	https://github.com/owncloud/security-advisories/security/advisories/GHSA-4m66-rpfj-m5f6
https://nvd.nist.gov/vuln/detail/CVE-2026-8377	8,2	Access Control System (GKS)	Missing Authorization	Access Control System (GKS): before Version 2	https://siberguvenlik.gov.tr/guvenlik-bildirimleri/detay/tr-26-0502
https://nvd.nist.gov/vuln/detail/CVE-2026-14476	8,0	SSSD's AD GPO provider	Relative Path Traversal	SSSD's AD GPO provider	https://access.redhat.com/security/cve/CVE-2026-14476 https://bugzilla.redhat.com/show_bug.cgi?id=2496581
https://nvd.nist.gov/vuln/detail/CVE-2026-25271	7,8	Qualcomm, Inc.	Time-of-check Time-of-use (TOCTOU) Race Condition	Qualcomm, Inc.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2026-bulletin.html
https://nvd.nist.gov/vuln/detail/CVE-2026-6509	7,8	Pardus Update	Missing Authorization	Pardus Update: from <=0.6.3 before 0.6.6	https://siberguvenlik.gov.tr/guvenlik-bildirimleri/detay/tr-26-0501
https://nvd.nist.gov/vuln/detail/CVE-2026-9165	7,7	Red Hat Advanced Cluster Security for Kubernetes (RHACS)	Uncontrolled Resource Consumption	Red Hat Advanced Cluster Security for Kubernetes (RHACS)	https://access.redhat.com/security/cve/CVE-2026-9165 https://bugzilla.redhat.com/show_bug.cgi?id=2480505
https://nvd.nist.gov/vuln/detail/CVE-2026-24012	7,5	Apache IoTDB	Uncontrolled Resource Consumption	Apache IoTDB: from 1.3.3 before 2.0.8	http://www.openwall.com/lists/oss-security/2026/07/06/10 https://lists.apache.org/thread/0g5th1t2vj6j8hm5t9w3xh9n6f6ht9z8
https://nvd.nist.gov/vuln/detail/CVE-2026-54234	7,5	vLLM	Improper Input Validation	vLLM prior to 0.24.0	https://github.com/vllm-project/vllm/commit/8a5cf1ccd65e8ac7635c402c1ec0b08988bc26ca https://github.com/vllm-project/vllm/pull/44744 https://github.com/vllm-project/vllm/security/advisories/GHSA-8wr5-jm2h-8r4f
https://nvd.nist.gov/vuln/detail/CVE-2026-55380	7,5	Pillow	Memory Allocation with Excessive Size Value	Pillow Prior to 12.3.0	https://github.com/python-pillow/Pillow/blob/main/docs/releasenotes/12.3.0.rst https://github.com/python-pillow/Pillow/commit/f39b0ae6624eb2d7c5c5d651d9bb5fdbd96a8675 https://github.com/python-pillow/Pillow/security/advisories/GHSA-phj9-mv4w-65pm
https://nvd.nist.gov/vuln/detail/CVE-2026-55727	7,5	Genetec Security Center	Improper Authentication	Genetec Security Center 5.14.0.0 prior to build 5.14.178.18	https://resources.genetec.com/security-advisories/vulnerability-affecting-live-video-retrieval-in-security-center-5-14-0-0
https://nvd.nist.gov/vuln/detail/CVE-2026-55994	7,5	Apache Camel	Improper Input Validation	Apache Camel: from 4.17.0 before 4.18.3, from 4.19.0 before 4.21.0	http://www.openwall.com/lists/oss-security/2026/07/05/28 https://camel.apache.org/security/CVE-2026-55994.html
https://nvd.nist.gov/vuln/detail/CVE-2026-5730	7,5	Ontime	Authorization Bypass Through User-Controlled Key	Ontime: through 04052026.	https://siberguvenlik.gov.tr/guvenlik-bildirimleri/detay/tr-26-0503
https://nvd.nist.gov/vuln/detail/CVE-2026-5799	7,5	Ontime	Authorization Bypass Through User-Controlled Key	Ontime: through 04052026	https://siberguvenlik.gov.tr/guvenlik-bildirimleri/detay/tr-26-0503
https://nvd.nist.gov/vuln/detail/CVE-2026-14642	7,3	SourceCodester Class and Exam	Improper Neutralization of Special Elements in Output Used by a	SourceCodester Class and Exam Timetabling System 1.0	https://github.com/sunjingyuan123/ccvvee/issues/1 VulDB https://vuldb.com/cve/CVE-2026-14642 VulDB https://vuldb.com/submit/846144

		Timetabling System 1.0	Downstream Component ('Injection')		https://vuldb.com/vuln/376158 https://vuldb.com/vuln/376158/cti https://www.sourcecodester.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-14648	7,3	Online Voting System	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	Online Voting System up to 0.x/1.0	https://code-projects.org/ VulDB https://gist.github.com/c4ttr4ck/ed954dc2e3da968eb460a18385146f4c VulDB https://vuldb.com/cve/CVE-2026-14648 https://vuldb.com/submit/846328 https://vuldb.com/vuln/376161 https://vuldb.com/vuln/376161/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-14764	7,3	Hotel and Tourism Reservation 1.0	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	Hotel and Tourism Reservation 1.0	https://code-projects.org/ VulDB https://raw.githubusercontent.com/anubhavv106/Security-Advisories/refs/heads/main/Hotel-Tourism-Reservation-add_event.php_SQLi.md VulDB https://vuldb.com/cve/CVE-2026-14764 https://vuldb.com/submit/850582 https://vuldb.com/vuln/376353 https://vuldb.com/vuln/376353/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-14802	7,3	create-react-app	Improper Neutralization of Special Elements used in a Command ('Command Injection')	create-react-app up to 5.0.1 on macOS	https://github.com/react/create-react-app/ VulDB https://github.com/react/create-react-app/issues/17269 VulDB https://vuldb.com/cve/CVE-2026-14802 https://vuldb.com/submit/850857 https://vuldb.com/vuln/376396 https://vuldb.com/vuln/376396/cti
https://nvd.nist.gov/vuln/detail/CVE-2026-49042	7,3	Apache Camel	Improper Input Validation	Apache Camel: from 4.8.0 through 4.18.2, from 4.19.0 through 4.20.0	http://www.openwall.com/lists/oss-security/2026/07/06/17 https://camel.apache.org/security/CVE-2026-49042.html
https://nvd.nist.gov/vuln/detail/CVE-2026-58380	7,3	GIMP's PNM file format parser	Off-by-one Error	GIMP's PNM file format parser	https://access.redhat.com/security/cve/CVE-2026-58380 https://bugzilla.redhat.com/show_bug.cgi?id=2496135 https://gitlab.gnome.org/GNOME/gimp/-/commit/83699817 https://gitlab.gnome.org/GNOME/gimp/-/issues/16206
https://nvd.nist.gov/vuln/detail/CVE-2026-58384	7,3	GIMP's PSD parser	Integer Overflow or Wraparound	GIMP's PSD parser	https://access.redhat.com/security/cve/CVE-2026-58384 https://bugzilla.redhat.com/show_bug.cgi?id=2497431 https://gitlab.gnome.org/GNOME/gimp/-/commit/da29e217 https://gitlab.gnome.org/GNOME/gimp/-/issues/16216
https://nvd.nist.gov/vuln/detail/CVE-2026-13705	7,1	Imager versions	Out-of-bounds Read	Imager versions before 1.032 for Perl	http://www.openwall.com/lists/oss-security/2026/07/06/3 https://github.com/tonycoz/imager/commit/f28de02770dfc26ffbdc32048970ed84babbf730.patch https://metacpan.org/release/TONYC/Imager-1.032/source/Changes
https://nvd.nist.gov/vuln/detail/CVE-2026-21383	7,1	Qualcomm, Inc.	Reusing a Nonce, Key Pair in Encryption	Qualcomm, Inc.	https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2026-bulletin.html

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
Vulnerability Summary for the Week of June 29, 2026		https://www.cisa.gov/news-events/bulletins/sb26-187

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
Windows Device Identifier Feature Leads to Arrest of Scattered Spider Hacking Group Member	https://cybersecuritynews.com/windows-device-identifier-tracking/
The Gentlemen Ransomware Uses 21 Remote Execution Techniques to Encrypt Entire Networks	https://cybersecuritynews.com/the-gentlemen-ransomware-uses-21-remote-execution-techniques/
SilverFox Hackers Use Go RAT, AV Killer, and Kernel Rootkit in Live ValleyRAT Campaign	https://cybersecuritynews.com/silverfox-hackers-use-go-rat-av-killer/
15-Year-Old Arrested Over Bandai Channel Cyberattack Using a ChatGPT-Assisted Tool	https://cybersecuritynews.com/bandai-channel-cyberattack/
Indian Govt Bans Apps Being Misused to Stop E-Rickshaws Remotely	https://cybersecuritynews.com/indian-govt-bans-e-rickshaws-apps/
Cyber Security News Bulletin Weekly – Mythos is Back, WhatsApp Username, Kali Linux 2026.2, +20 Stories	https://cybersecuritynews.com/cyber-security-news-bulletin-weekly/

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
Hackers Abuse 2026 FIFA World Cup Hype to Harvest PII and Payment Card Details	https://cybersecuritynews.com/hackers-abuse-2026-fifa-world-cup-hype/
Moody Bible Institute Data Breach Exposes 2.3 Million Users' Personal Data	https://cybersecuritynews.com/moody-bible-institute-data-breach/
RedLine C2 Pivot Reveals Seven Fraudulent Domains Used in Maritime Phishing Attacks	https://cybersecuritynews.com/redline-c2-pivot-reveals-seven-fraudulent-domains/

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
OpenAI Codex Desktop App for macOS Vulnerability Allows Attackers to Inject Indirect Prompt	https://cybersecuritynews.com/codex-desktop-app-for-macos-vulnerability/
16-Year-Old Linux KVM Vulnerability Allows Malicious Guest to Corrupt Host Kernel Memory	https://cybersecuritynews.com/16-year-old-linux-kvm-vulnerability/
Critical BeyondTrust Flaws Let Attackers Bypass Access Controls and Gain Unauthorized Access	https://cybersecuritynews.com/beyondtrust-vulnerabilities/
Fast-mcp-telegram Vulnerability Allow Attackers to Access Sensitive Files	https://cybersecuritynews.com/fast-mcp-telegram-vulnerability/
Microsoft Device Code Phishing Attack Steals Tokens Through Legitimate Login Page	https://cybersecuritynews.com/microsoft-device-code-phishing-attack/
Gemini Live Voice Session Flaw Enables Tool Injection Through Misconfigured Ephemeral Tokens	https://cybersecuritynews.com/gemini-live-voice-session-flaw/
Microsoft Edge Vulnerability Allows Remote Attacker to Execute Arbitrary Code	https://cybersecuritynews.com/microsoft-edge-flaw-code-execution/
Windows 11 24H2 and 25H2 Issue Causes Black Screen, Start Menu Failure, and Taskbar Crashes	https://cybersecuritynews.com/windows-11-24h2-and-25h2-issues/
Multiple IBM WebSphere Vulnerabilities Enable XSS and Path Traversal Attacks	https://cybersecuritynews.com/ibm-websphere-vulnerabilities/
Multiple PHP Vulnerabilities Enable DoS and Memory Corruption Attacks	https://cybersecuritynews.com/multiple-php-vulnerabilities-dos/
Multiple ModSecurity Vulnerabilities Allow Attackers to Bypass Firewall Rules	https://cybersecuritynews.com/modsecurity-vulnerabilities/
Opera GX 0-Click Vulnerability Lets Attackers Exfiltrate User Data via Malicious Website	https://cybersecuritynews.com/opera-gx-0-click-vulnerability/
T3MP3ST Security Framework With 35 Tools, Turns AI Coding Agents Into 0-Day Bug Hunters	https://cybersecuritynews.com/t3mp3st-security-framework/
Multiple FatFs Vulnerabilities Expose Millions of Embedded Devices to Cyber Risks	https://cybersecuritynews.com/fatfs-vulnerabilities/
New “Bad Epoll” 0-Day Vulnerability Allows Root Access on Linux Servers and Android Devices	https://cybersecuritynews.com/bad-epoll-0-day-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
OpenSSH 10.4 Released with Multiple Security Fixes and New Features	https://cybersecuritynews.com/openssh-10-4-security-fixes/
Parrot 7.3 Released With Optimized Packages and Updated Tools	https://cybersecuritynews.com/parrot-7-3-released/
Flipper Zero Firmware Development Continues With New Community Contribution Rules	https://cybersecuritynews.com/flipper-zero-firmware-development/
Microsoft Releases OOBE Cumulative Update for Windows 11, Versions 24H2 and 25H2	https://cybersecuritynews.com/windows-11-oobe-cumulative-update/

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
Hackers Leverage Microsoft Teams Call to Install RMM Tools and Deploy EtherRAT	https://cybersecuritynews.com/hackers-leverage-microsoft-teams-call/
Cavern Manticore Abuses SysAid RMM and WinDirStat DLL Sideloading to Deploy C2 Framework	https://cybersecuritynews.com/cavern-manticore-abuses-sysaid-rmm-and-windirstat-dll-sideloading/
Tenda Authentication Backdoor Grants Attackers Full Administrative Access	https://cybersecuritynews.com/tenda-authentication-backdoor-grants-access/
Agent Skill Malware Targets Claude Code and OpenAI Codex With Scanner-Evasion Techniques	https://cybersecuritynews.com/agent-skill-malware-targets-claude-code-and-openai-codex/
Gaslight macOS Malware Uses Prompt Injection to Evade AI Security Analysis	https://cybersecuritynews.com/gaslight-macos-malware-uses-prompt-injection/
TrojPix Attacks Allow Hackers to Access Data from Air-gapped Computers from 208 Meters	https://cybersecuritynews.com/trojpix-attack/
Hackers Abuse OpenAI Org Invites to Harvest Sensitive Prompts and API Activity	https://cybersecuritynews.com/hackers-use-openai-org-invites/
SSH Honeypots Miss Most Post-Login Attacks by Focusing on Interactive Shells	https://cybersecuritynews.com/ssh-honeypots-miss-most-post-login-attacks/
PamStealer Mimics Maccy Clipboard Manager Silently Harvests Data and Clipboard Contents	https://cybersecuritynews.com/pamstealer-mimic-as-maccy-harvest/

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
The Business Cost of Alert Fatigue: How to Reduce Delays, Escalations for Your SOC as 70% Alerts are Un-investigated	https://cybersecuritynews.com/the-business-cost-of-alert-fatigue/
Top Tools for Enterprise Security Monitoring	https://cybersecuritynews.com/enterprise-security-monitoring-tools/
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
Top 10 Best Next-Generation Firewall (NGFW) Solutions in 2026	https://cybersecuritynews.com/best-next-generation-firewall/

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/