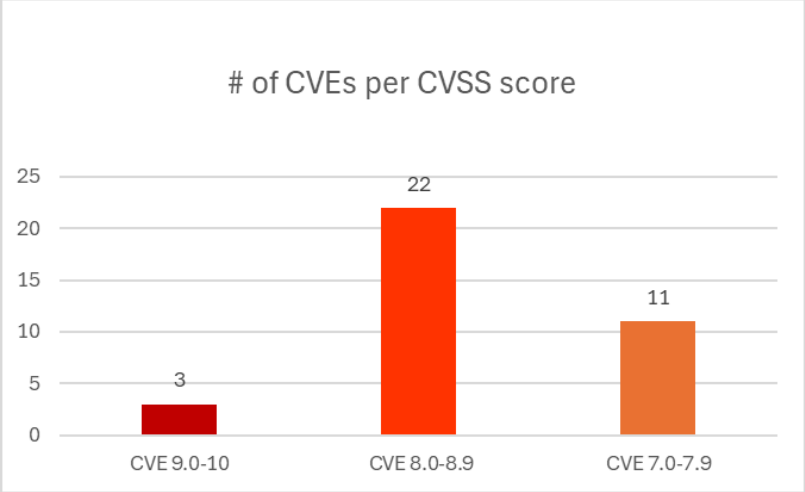
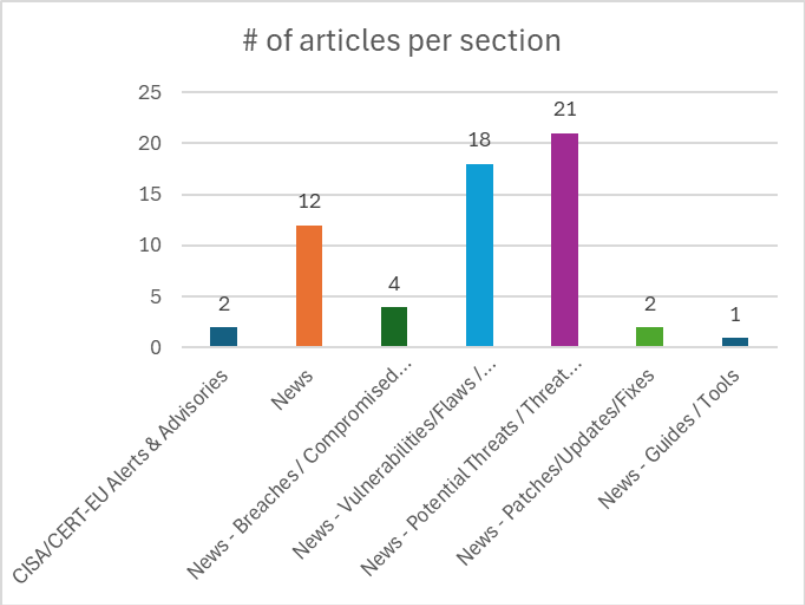
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 20/02/2026 - 24/02/2026





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)	CVSSv 3	Προϊόν/Υπη-ρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2026-27211	10,0	Cloud Hypervisor	External Control of File Name or Path	Versions 34.0 through 50.0	https://github.com/cloud-hypervisor/cloud-hypervisor/commit/081a6ebb5184228ff348601502258f3f72bd8b43 https://github.com/cloud-hypervisor/cloud-hypervisor/commit/509832298b6865365b00bda88722e76e41ce7f41 https://github.com/cloud-hypervisor/cloud-hypervisor/commit/a63315df54e06f6ec867f17b63076c266e2d8648 https://github.com/cloud-hypervisor/cloud-hypervisor/commit/cb495959a8bea1b56e8fc82d15ba527a0e7fcf3c https://github.com/cloud-hypervisor/cloud-hypervisor/releases/tag/v50.1 https://github.com/cloud-hypervisor/cloud-hypervisor/releases/tag/v51.0 https://github.com/cloud-hypervisor/cloud-hypervisor/security/advisories/GHSA-jmr4-g2hv-mjj6
https://nvd.nist.gov/vuln/detail/CVE-2026-27507	9,8	Binardat	Binardat 10G08-0800GSM network switch firmware version V300SP10260209 and prior	Use of Hard-coded Credentials	https://www.binardat.com/products/8-port-10-gigabit-sfp-managed-switch,-support-1g-sfp-and-10g-sfp-module,-160gbps-bandwidth,-l3-web-managed,-metal-fanless-fiber-binardat-network-switch https://www.vulncheck.com/advisories/binardat-10g08-0800gsm-network-switch-hard-coded-credentials
https://nvd.nist.gov/vuln/detail/CVE-2026-27515	9,1	Binardat	Binardat 10G08-0800GSM network switch firmware versions prior to V300SP10260209	Use of Insufficiently Random Values	https://www.binardat.com/products/8-port-10-gigabit-sfp-managed-switch,-support-1g-sfp-and-10g-sfp-module,-160gbps-bandwidth,-l3-web-managed,-metal-fanless-fiber-binardat-network-switch https://www.vulncheck.com/advisories/binardat-10g08-0800gsm-network-switch-predictable-session-identifiers
https://nvd.nist.gov/vuln/detail/CVE-2025-13943	8,8	Zyxel	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Zyxel EX3301-T0	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-null-pointer-dereference-and-command-injection-vulnerabilities-in-certain-4g-lte-5g-nr-cpe-dsl-ethernet-cpe-fiber-onts-security-routers-and-wireless-extenders-02-24-2026
https://nvd.nist.gov/vuln/detail/CVE-2026-2041	8,8	Nagios	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Nagios Host zabbix-agent_configwizard_func Command Injection Remote Code Execution Vulnerability	https://www.nagios.com/changelog/nagios-xi/nagios-xi-2026r1-0-1/ https://www.zerodayinitiative.com/advisories/ZDI-26-073/

https://nvd.nist.gov/vuln/detail/CVE-2026-2043	8,8	Nagios	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Nagios Host esensors_websensor_config-wizard_func Command Injection Remote Code Execution Vulnerability	https://www.nagios.com/changelog/nagios-xi/nagios-xi-2026r1-0-1/ https://www.zerodayinitiative.com/advisories/ZDI-26-072/
https://nvd.nist.gov/vuln/detail/CVE-2026-23678	8,8	Binardat	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Binardat 10G08-0800GSM network switch firmware version V300SP10260209 and prior	https://www.binardat.com/products/8-port-10-gigabit-sfp-managed-switch,-support-1g-sfp-and-10g-sfp-module,-160gbps-bandwidth,-l3-web-managed,-metal-fanless-fiber-binardat-network-switch https://www.vulncheck.com/advisories/binardat-10g08-0800gsm-network-switch-traceroute-cli-command-injection
https://nvd.nist.gov/vuln/detail/CVE-2026-2769	8,8	Firefox, Thunderbird	Use After Free	Firefox < 148, Firefox ESR < 115.33, Firefox ESR < 140.8, Thunderbird < 148, and Thunderbird < 140.8	https://bugzilla.mozilla.org/show_bug.cgi?id=2014550 Mozilla Corporation https://www.mozilla.org/security/advisories/mfsa2026-13/ https://www.mozilla.org/security/advisories/mfsa2026-14/ https://www.mozilla.org/security/advisories/mfsa2026-15/ https://www.mozilla.org/security/advisories/mfsa2026-16/ https://www.mozilla.org/security/advisories/mfsa2026-17/
https://nvd.nist.gov/vuln/detail/CVE-2026-2798	8,8	Firefox, Thunderbird	Use After Free	Firefox < 148 and Thunderbird < 148	https://bugzilla.mozilla.org/show_bug.cgi?id=2014136 https://www.mozilla.org/security/advisories/mfsa2026-13/ https://www.mozilla.org/security/advisories/mfsa2026-16/
https://nvd.nist.gov/vuln/detail/CVE-2026-2824	8,8	Comfast	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Comfast CF-E7 2.6.0.9	https://github.com/jinhao118/cve/blob/main/ComFast%20Router_4.md https://vuldb.com/?ctiid.346949 https://vuldb.com/?id.346949 https://vuldb.com/?submit.753878
https://nvd.nist.gov/vuln/detail/CVE-2026-2874	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda A21 1.0.0.0	https://github.com/QIU-DIE/cve-nneeww/issues/5 https://vuldb.com/?ctiid.347111 https://vuldb.com/?id.347111 https://vuldb.com/?submit.754636 https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-2877	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda A18 15.13.07.13	https://github.com/master-abc/cve/issues/39 https://vuldb.com/?ctiid.347130 https://vuldb.com/?id.347130 https://vuldb.com/?submit.754703 https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-2886	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda A21 1.0.0.0	https://github.com/QIU-DIE/cve-nneeww/issues/6 https://vuldb.com/?ctiid.347180 https://vuldb.com/?id.347180 https://vuldb.com/?submit.754640 https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-2904	8,8	UTT	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	UTT HiPER 810G 1.7.7-171114	https://vuldb.com/?ctiid.347213 https://vuldb.com/?id.347213 https://vuldb.com/?submit.755113 https://vuln.ricky.place/UTT/HiPER%20810G/

https://nvd.nist.gov/vuln/detail/CVE-2026-2910	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda HG9 300001138	https://github.com/QIU-DIE/cve-nneeww/issues/12 https://vuldb.com/?ctiid.347219 https://vuldb.com/?id.347219 https://vuldb.com/?submit.755212 https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-2911	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda FH451 up to 1.0.0.9	https://vuldb.com/?ctiid.347220 https://vuldb.com/?id.347220 https://vuldb.com/?submit.755218 https://vuln.ricky.place/Tenda/FH451/ https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-2930	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda A18 15.13.07.13	https://github.com/master-abc/cve/issues/40 https://vuldb.com/?ctiid.347277 https://vuldb.com/?id.347277 https://vuldb.com/?submit.755227 https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-2961	8,8	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	D-Link DWR-M960 1.01.07	https://github.com/LX-66-LX/cve-new/issues/28 https://vuldb.com/?ctiid.347328 https://vuldb.com/?id.347328 https://vuldb.com/?submit.754513 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-2962	8,8	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	D-Link DWR-M960 1.01.07	https://github.com/LX-66-LX/cve-new/issues/29 https://vuldb.com/?ctiid.347329 https://vuldb.com/?id.347329 https://vuldb.com/?submit.754517 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-3016	8,8	UTT	Improper Restriction of Operations within the Bounds of a Memory Buffer	UTT HiPER 810G up to 1.7.7-171114	https://github.com/xhsy0314/CVEReport/blob/main/UTT-2/README.md https://github.com/xhsy0314/CVEReport/blob/main/UTT-2/README.md#poc https://vuldb.com/?ctiid.347376 https://vuldb.com/?id.347376 https://vuldb.com/?submit.756249
https://nvd.nist.gov/vuln/detail/CVE-2026-3044	8,8	Tenda	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda AC8 16.03.34.06	https://github.com/master-abc/cve/issues/43 https://vuldb.com/?ctiid.347400 https://vuldb.com/?id.347400 https://vuldb.com/?submit.757240 https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-27203	8,3	eBay API MCP Server	External Control of System or Configuration Setting		https://github.com/YosefHayim/ebay-mcp/commit/aab0bda75ea9dd27aa37d0d8524d7cf41b3c4a9a https://github.com/YosefHayim/ebay-mcp/security/advisories/GHSA-97rm-xj73-33jh
https://nvd.nist.gov/vuln/detail/CVE-2026-2818	8,2	Spring Data	Relative Path Traversal		https://www.herodevs.com/vulnerability-directory/cve-2026-2818
https://nvd.nist.gov/vuln/detail/CVE-2026-27134	8,1	Strimzi	Improper Authentication	versions 0.49.0 through 0.50.0	https://github.com/strimzi/strimzi-kafka-operator/releases/tag/0.50.1 https://github.com/strimzi/strimzi-kafka-operator/security/advisories/GHSA-2qwx-rq6j-8r6j

https://nvd.nist.gov/vuln/detail/CVE-2025-70329	8,0	TOTOLink	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	TOTOLink X5000R v9.1.0cu_2415_B20250515	https://github.com/neighborhood-H/0-DAY/blob/main/Toto-link/X5000R/SetIptvCfg/report.md https://www.notion.so/TOTOLINK-X5000R-SetIptvCfg-2d170566ca7f8027ad47e6b5429025fc?source=copy_link
https://nvd.nist.gov/vuln/detail/CVE-2026-21420	7,8	Dell	Uncontrolled Search Path Element	Dell Repository Manager (DRM), versions prior to 3.4.8	https://www.dell.com/support/kbdoc/en-us/000430183/dsa-2026-059-security-update-for-dell-repository-manager-vulnerability
https://nvd.nist.gov/vuln/detail/CVE-2026-2998	7,8	ERP developed by eAI Technologies	Untrusted Search Path		https://www.twcert.org.tw/en/cp-139-10723-14549-2.html https://www.twcert.org.tw/tw/cp-132-10722-db7cb-1.html
https://nvd.nist.gov/vuln/detail/CVE-2025-69700	7,5	Tenda	Stack-based Buffer Overflow	Tenda FH1203 V2.0.1.6	https://github.com/xhh0124/SemVulLLM
https://nvd.nist.gov/vuln/detail/CVE-2026-24892	7,5	openITCOCKPIT	Deserialization of Untrusted Data	openITCOCKPIT Community Edition 5.3.1	https://github.com/openITCOCKPIT/openITCOCKPIT/commit/975e0d0dfb79898568afbbfdba8f647d92612a69 https://github.com/openITCOCKPIT/openITCOCKPIT/releases/tag/openITCOCKPIT-5.4.0 https://github.com/openITCOCKPIT/openITCOCKPIT/security/advisories/GHSA-g83p-vvjm-g39x
https://nvd.nist.gov/vuln/detail/CVE-2026-26048	7,5	Wi-Fi router	Missing Authentication for Critical Function		https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-050-03.json https://www.cisa.gov/news-events/ics-advisories/icsa-26-050-03
https://nvd.nist.gov/vuln/detail/CVE-2026-27520	7,5	Binardat	Cleartext Storage of Sensitive Information	Binardat 10G08-0800GSM network switch firmware versions prior to V300SP10260209	https://www.binardat.com/products/8-port-10-gigabit-sfp-managed-switch,-support-1g-sfp-and-10g-sfp-module,-160gbps-bandwidth,-l3-web-managed,-metal-fanless-fiber-binardat-network-switch https://www.vulncheck.com/advisories/binardat-10g08-0800gsm-network-switch-base64-encoded-password-stored-in-cookie
https://nvd.nist.gov/vuln/detail/CVE-2025-33181	7,3	NVIDIA Cumulus Linux and NVOS products	Improper Neutralization of Special Elements used in a Command ('Command Injection')		https://nvd.nist.gov/vuln/detail/CVE-2025-33181 https://nvidia.custhelp.com/app/answers/detail/a_id/5722 https://www.cve.org/CVERecord?id=CVE-2025-33181
https://nvd.nist.gov/vuln/detail/CVE-2026-3053	7,3	DataLinkDC	Improper Authentication	DataLinkDC dinky up to 1.2.5	https://github.com/AnalogyC0de/public_exp/issues/6 https://github.com/AnalogyC0de/public_exp/issues/6#issue-3935019636 https://vuldb.com/?ctiid.347411 https://vuldb.com/?id.347411 https://vuldb.com/?submit.757589
https://nvd.nist.gov/vuln/detail/CVE-2026-1459	7,2	Zyxel	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Zyxel VMG3625-T50B firmware versions through 5.50(ABPM.9.7)C0	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-null-pointer-dereference-and-command-injection-vulnerabilities-in-certain-4g-lte-5g-nr-cpe-dsl-ether-net-cpe-fiber-onts-security-routers-and-wireless-extenders-02-24-2026
https://nvd.nist.gov/vuln/detail/CVE-2026-22766	7,2	Dell	Unrestricted Upload of File with Dangerous Type	Dell Wyse Management Suite, versions prior to WMS 5.5	https://www.dell.com/support/kbdoc/en-us/000429141/dsa-2026-103

https://nvd.nist.gov/vuln/detail/CVE-2026-2847	7,2	UTT	Improper Neutralization of Special Elements used in a Command ('Command Injection')	UTT HiPER 520 1.7.7-160105	https://github.com/cha0yang1/UTT520CVE/blob/main/UTTRCE2.md https://vuldb.com/?ctiid.347083 https://vuldb.com/?id.347083 https://vuldb.com/?submit.753965

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 Two Known Exploited Vulnerabilities to Catalog	▪ CVE-2025-49113 RoundCube Webmail Deserialization of Untrusted Data Vulnerability ▪ CVE-2025-68461 RoundCube Webmail Cross-site Scripting Vulnerability	https://www.cisa.gov/news-events/alerts/2026/02/20/cisa-adds-two-known-exploited-vulnerabilities-catalog
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2026-25108 Soliton Systems K.K. FileZen OS Command Injection Vulnerability	https://www.cisa.gov/news-events/alerts/2026/02/24/cisa-adds-one-known-exploited-vulnerability-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
US Sanctions Network of Exploit Brokers That Stole US Government Cyber Tools	https://cybersecuritynews.com/us-sanctions-exploit-brokers/
65% of Financial Organizations Targeted by Ransomware as Cybercriminals Escalate Attacks	https://cybersecuritynews.com/financial-organizations-ransomware-attack-2024/
Elon Musk Accuses Anthropic of Stealing Data in a Massive Scale	https://cybersecuritynews.com/elon-musk-accuses-anthropic/
OpenClaw Releases 2026.2.23 Released With Security Updates and New AI features	https://cybersecuritynews.com/openclaw-2026-2-23-released/
Google Suspends OpenClaw Users from Antigravity AI After OAuth Token Abuse	https://cybersecuritynews.com/google-suspends-openclaw-users/
Google Blocked 1.75 Million Malicious Apps from Entering into the Play Store	https://cybersecuritynews.com/google-blocked-1-75-million-malicious-apps-from-play-store/
Cybersecurity News Weekly: PayPal Breach, Chrome 0-Day, BeyondTrust RCE Exploit, and More	https://cybersecuritynews.com/cybersecurity-news-weekly/
Multiple Hacking Groups Exploit OpenClaw Instances to Steal API key and Deploy Malware	https://cybersecuritynews.com/hacking-groups-exploit-openclaw/
Cloudflare Down – 6 Hour of Massive Global Service Outage Cause Customers Unreachable From the Internet	https://cybersecuritynews.com/cloudflare-down-6-hour-of-massive-global-service-outage/
Hackers Leveraging Multiple AI Services to Compromise 600+ FortiGate Devices	https://cybersecuritynews.com/600-fortigate-devices-hacked/
Silicon Valley Engineers Charged With Stealing Trade Secrets From Google and Other Tech Companies	https://cybersecuritynews.com/silicon-valley-engineers-charged/
Hackers Using OAuth Apps in Microsoft Entra ID to Establish Persistence	https://cybersecuritynews.com/microsoft-entra-id-for-persistence/

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
Conduent Data Breach – Largest Data Breach in U.S. History As Ransomware Group Stolen 8 TB of Data	https://cybersecuritynews.com/conduent-data-breach/
ShinyHunters Allegedly Claim Breach of 21 Million Records from Odido	https://cybersecuritynews.com/shinyhunters-claim-breach-odido/
Threat Actor Allegedly Claimed Leak of Wendy's International Franchise Database	https://cybersecuritynews.com/wendy-data-breach/
PayPal Data Breach Exposes SSNs and Business PII of Customers for Over Six Months	https://cybersecuritynews.com/paypal-data-breach-expose-customer-data/

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
Multiple Vulnerabilities in CPSD CryptoPro Secure Disk for BitLocker Allow Root Access and Credential Theft	https://cybersecuritynews.com/vulnerabilities-in-cpsd-cryptopro-secure-disk-for-bitlocker/
GitHub Copilot Exploited to Perform Full Repository Takeover via Passive Prompt Injection	https://cybersecuritynews.com/github-copilot-exploited/
New Deserialization Vulnerability in Ruby Workers Could Enable Full System Compromise	https://cybersecuritynews.com/deserialization-vulnerability-in-ruby/
Multiple VMware Aria Vulnerabilities Allow Remote Code Execution Attacks	https://cybersecuritynews.com/vmware-aria-vulnerabilities-rce-attack/
Google Chrome Emergency Security Update Patches Three High-Severity Vulnerabilities	https://cybersecuritynews.com/google-chrome-emergency-security-update/
PoC Exploit Released for Grandstream GXP1600 VoIP Phones RCE Vulnerability	https://cybersecuritynews.com/grandstream-gxp1600-voip-phones-rce-vulnerability/
jsPDF Vulnerability Exposes Millions of Developers to Object Injection Attacks	https://cybersecuritynews.com/jspdf-vulnerability-injection-attacks/
HPE Telco Service Activator Vulnerability Let Attackers Bypass Access Restrictions	https://cybersecuritynews.com/hpe-telco-service-activator-vulnerability/
CISA Warns of Multiple Roundcube Vulnerabilities Exploited in Attacks	https://cybersecuritynews.com/roundcube-vulnerabilities-exploited/
OWASP Smart Contract Top 10 2026 — Security Risks and Vulnerabilities	https://cybersecuritynews.com/owasp-smart-contract-top-10-2026/
New Shai-Hulud–like npm Worm Attack 19+ Packages to Steal dev/CI Secrets	https://cybersecuritynews.com/shai-hulud-like-npm-worm-attack/
Critical Jenkins Vulnerability Exposes Build Environments to XSS Attacks	https://cybersecuritynews.com/jenkins-vulnerability-exposes-xss-attacks/
Apache Tomcat Vulnerabilities Let Attackers Bypass Security Constraints via HTTP/0.9 Requests	https://cybersecuritynews.com/apache-tomcat-bypass-vulnerabilities/
Critical Vulnerabilities in VS Code Extensions Threaten 128 Million Developer Environments	https://cybersecuritynews.com/popular-vs-code-extensions-vulnerability/
PoC Released for Critical Chrome 0-day Vulnerability Exploited in the Wild	https://cybersecuritynews.com/chrome-0-day-vulnerability-poc/
PoC Released for Windows Notepad Vulnerability that Enables Malicious Command Execution	https://cybersecuritynews.com/poc-windows-notepad-vulnerability/
Google Issues Emergency Chrome Security Update to Address High-Severity PDFium and V8 Flaws	https://cybersecuritynews.com/chrome-emergency-security-update/
Splunk Enterprise for Windows Vulnerability Let Attackers Hijack DLLs and Gain SYSTEM Access	https://cybersecuritynews.com/splunk-enterprise-for-windows-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
Microsoft Released Updates for Windows 11, Version 25H2 and 24H2 Systems	https://cybersecuritynews.com/microsoft-released-updates-for-windows-11-25h2-and-24h2/
WhatsApp Introduces Optional Account Password Feature to Strengthen Login Security	https://cybersecuritynews.com/whatsapp-password-feature/

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
Microsoft Warns of Hackers Attacking Developers with Malicious Next.js Repositories	https://cybersecuritynews.com/malicious-next-js-repositories/
Threat Actors Exploit Apache ActiveMQ Server Vulnerability to Gain RDP Access and Deploy LockBit Ransomware	https://cybersecuritynews.com/threat-actors-exploit-apache-activemq-server-vulnerability/
Threat Actors Weaponized AI Tools to Gain Full Domain Access within 30 Minutes	https://cybersecuritynews.com/threat-actors-weaponized-ai-tools/
Malicious NuGet Packages Attacking ASP.NET Developers to Steal Login Credentials	https://cybersecuritynews.com/malicious-nuget-packages-attacking/
Malicious OpenClaw Skills Used to Trick Users into Manual Password Entry for AMOS Infection	https://cybersecuritynews.com/malicious-openclaw-skills-used/
Hackers Leverage Steganographic Images to Bypass Anti-Malware Scans and Deploy Malware Payloads	https://cybersecuritynews.com/hackers-leverage-steganographic-images/
Fake Huorong Download Site Used to Deploy ValleyRAT Backdoor in Targeted Malware Campaign	https://cybersecuritynews.com/fake-huorong-download-site-used/
Diesel Vortex Russian Cybercrime Group Targets Global Logistics Sector and Steals 1,600+ Credentials	https://cybersecuritynews.com/diesel-vortex-targets-global-logistics-sector/
ClickFix Infostealer Campaign Uses Fake CAPTCHA Lures to Compromise Victims	https://cybersecuritynews.com/clickfix-infostealer-campaign/
Hackers Leverage DeepSeek and Claude to Attack FortiGate Devices Worldwide	https://cybersecuritynews.com/hackers-leverage-deepseek-and-claude/
GrayCharlie Injects Malicious JavaScript into WordPress Sites to Deliver NetSupport RAT and Stealc	https://cybersecuritynews.com/graycharlie-injects-malicious-javascript/
New MIMICRAT Custom RAT Uncovered in Sophisticated Multi-Stage ClickFix Campaign	https://cybersecuritynews.com/new-mimicrat-custom-rat-uncovered/
New Phishing Framework Starkiller Proxies Real Login Pages to Bypass MFA	https://cybersecuritynews.com/new-phishing-framework-starkiller-proxies/
North Korean Threat Actors Leverage Fake IT Worker Campaigns and Contagious Interview Tactics	https://cybersecuritynews.com/north-korean-threat-actors-leverage-fake-it-worker-campaigns/
DPRK Linked Operators Sustain Aggressive Crypto Targeting 12 Months After Bybit Breach	https://cybersecuritynews.com/aggressive-crypto-targeting-12-months-after-bybit-breach/

Silver Fox APT Uses DLL Sideloading and BYOVD Techniques in Sophisticated Malware Attacks	https://cybersecuritynews.com/silver-fox-apt-uses-dll-sideloading/
Grandstream VoIP Phones Vulnerability Allows Attackers to Gain Root Privileges	https://cybersecuritynews.com/grandstream-voip-phones-vulnerability/
CharlieKirk Grabber Stealer Attacking Windows Systems to Exfiltrate Login Credentials	https://cybersecuritynews.com/charliekirk-grabber-stealer-attacking-windows-systems/
LLM-Generated Passwords Expose Major Security Flaws with Predictability, Repetition, and Weakness	https://cybersecuritynews.com/llm-generated-passwords-expose-major-security-flaws/
Ploutus Malware Drains U.S. ATMs Without a Card or Account — FBI Issues Emergency FLASH Alert	https://cybersecuritynews.com/ploutus-malware-drains-u-s-atms/
Hackers Actively Exploiting Critical BeyondTrust Vulnerability to Deploy VShell and SparkRAT	https://cybersecuritynews.com/hackers-actively-exploiting-critical-beyondtrust-vulnerability/

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
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/