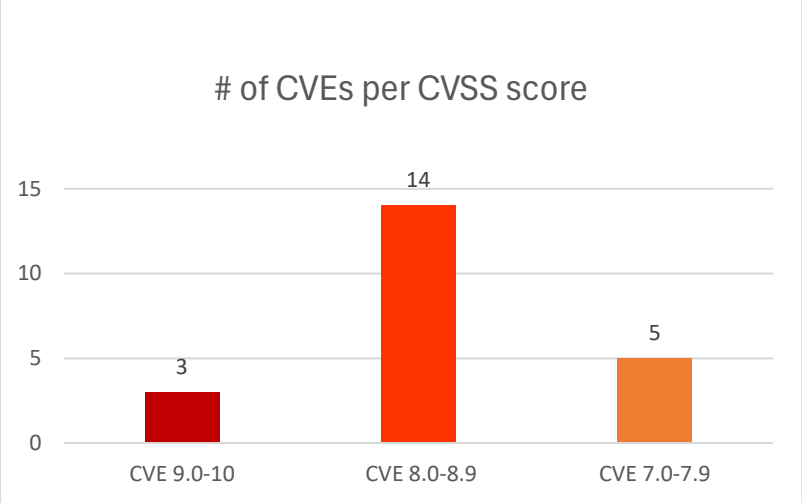
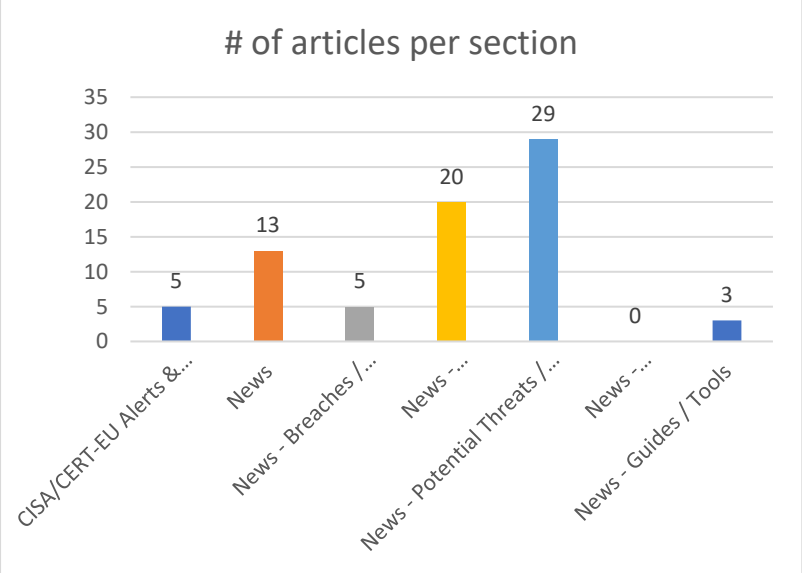
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 18/11/2025 - 21/11/2025





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/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2025-58083	10,0	Lynx+	Missing Authentication for Critical Function	General Industrial Controls Lynx+ Gateway is missing critical authentication in the embedded web server which could allow an attacker to remotely reset the device.	https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2025/icsa-25-317-08.json https://www.cisa.gov/news-events/ics-advisories/icsa-25-317-08
https://nvd.nist.gov/vuln/detail/CVE-2025-13188	9,8	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	A vulnerability was detected in D-Link DIR-816L 2_06_b09_beta. Affected by this vulnerability is the function authenticationcgi_main of the file /authentication.cgi.	https://github.com/scanleale/IOT_sec/blob/main/DIR-816L%20stack%20overflow(authentication.cgi).pdf https://vuldb.com/?ctiid.332476 https://vuldb.com/?id.332476 https://vuldb.com/?submit.685538 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2021-4470	9,3	TG8 Firewall	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	TG8 Firewall contains a pre-authentication remote code execution vulnerability in the runphpcmd.php endpoint.	https://ssd-disclosure.com/ssd-advisory-tg8-firewall-preauth-rce-and-password-disclosure/ https://web.archive.org/web/20211024224240/http://www.tg8security.com/ https://www.vulncheck.com/advisories/tg8-firewall-unauthenticated-rce-via-runphpcmd-php

https://nvd.nist.gov/vuln/detail/CVE-2025-13189	**8,8**	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	D-Link DIR-816L 2_06_b09_beta	https://github.com/scan-leale/IOT_sec/blob/main/DIR-816L%20stack%20overflow(gena.cgi).pdf https://vuldb.com/?ctiid.332478 https://vuldb.com/?id.332478 https://vuldb.com/?submit.685540 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-13190	**8,8**	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	A vulnerability was found in D-Link DIR-816L 2_06_b09_beta	https://github.com/scan-leale/IOT_sec/blob/main/DIR-816L%20stack%20overflow(scandir.sgi).pdf https://vuldb.com/?ctiid.332479 https://vuldb.com/?id.332479 https://vuldb.com/?submit.685541 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2016-15056	**8,7**	Ubee	Insertion of Sensitive Information into Externally-Accessible File or Directory	Ubee EVW3226 cable modem/routers firmware versions up to and including 1.0.20	https://seclists.org/fulldisclosure/2016/Jul/66 https://web.archive.org/web/20160403014231/http://www.ubeeinteractive.com/products/cable/evw3226 https://web.archive.org/web/20160726145043/http://www.search-lab.hu/advisories/122-ubee-evw3226-modem-router-multiple-vulnerabilities https://www.exploit-db.com/exploits/40156 https://www.vulncheck.com/advisories/ubee-evw3226-unauthenticated-backup-file-disclosure
https://nvd.nist.gov/vuln/detail/CVE-2018-25125	**8,7**	Netis ADSL Router	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	Netis ADSL Router DL4322D firmware RTK 2.1.1	https://web.archive.org/web/20180731191918/http://www.netis-systems.com/Home/detail/id/74.html https://www.exploit-db.com/exploits/45424 https://www.netis-systems.com/ https://www.vulncheck.com/advisories/netis-dl4322d-ftp-service-dos

https://nvd.nist.gov/vuln/detail/CVE-2021-4465	**8,7**	ReQuest	Uncontrolled Resource Consumption	ReQuest Serious Play F3 Media Server versions 7.0.3.4968 (Pro), 7.0.2.4954, 6.5.2.4954, 6.4.2.4681, 6.3.2.4203, and 2.0.1.823	http://www.request.com/ VulnCheck https://cxsecurity.com/issue/WLB-2020100122 CISA-ADP, VulnCheck https://exchange.xforce.ibmcloud.com/vulnerabilities/190031 https://packetstorm.news/files/id/159602 https://www.exploit-db.com/exploits/48951 https://www.vulncheck.com/advisories/request-serious-play-f3-media-server-remote-dos https://www.zeroscience.mk/en/vulnerabilities/ZSL-2020-5601.php
https://nvd.nist.gov/vuln/detail/CVE-2021-4467	**8,7**	Positive Technologies MaxPatrol	Uncontrolled Resource Consumption	Positive Technologies MaxPatrol 8 and XSpider contain a remote denial-of-service vulnerability in the client communication service on TCP port 2002.	https://cxsecurity.com/issue/WLB-2021090114 https://vulners.com/zdt/1337DAY-ID-36775 https://www.ptsecurity.com/ https://www.vulncheck.com/advisories/positive-technologies-maxpatrol-8-and-xspider-remote-dos
https://nvd.nist.gov/vuln/detail/CVE-2021-4468	**8,7**	PLANEX	Missing Authentication for Critical Function	PLANEX CS-QP50F-ING2 smart cameras expose a configuration backup interface over HTTP that does not require authentication.	https://cxsecurity.com/issue/WLB-2021010050 https://packetstorm.news/files/id/160805/ https://www.planex.co.jp/products/cs-qp50f/ https://www.vulncheck.com/advisories/planex-cs-qp50f-ing2-smart-camera-remote-configuration-disclosure
https://nvd.nist.gov/vuln/detail/CVE-2021-4469	**8,7**	Denver	Missing Authentication for Critical Function	Denver SHO-110 IP cameras expose a secondary HTTP service on TCP port 8001 that provides access to a '/snapshot' endpoint without authentication.	http://old.denver.eu/products/smart-home-security/denver-sho-110/c-1024/c-1243/p-3826 https://www.exploit-db.com/exploits/50162 https://www.vulncheck.com/advisories/denver-sho-110-ip-camera-unauthenticated-snapshot-access

https://nvd.nist.gov/vuln/detail/CVE-2021-4471	**8,7**	TG8 Firewall	Insertion of Sensitive Information into Externally-Accessible File or Directory	TG8 Firewall exposes a directory such as /data/ over HTTP without authentication.	https://ssd-disclosure.com/ssd-advisory-tg8-firewall-preauth-rce-and-password-disclosure/ https://web.archive.org/web/20211024224240/http://www.tg8security.com/ https://www.vulncheck.com/advisories/tg8-firewall-unauthenticated-user-password-disclosure
https://nvd.nist.gov/vuln/detail/CVE-2022-4985	**8,7**	Vodafone	Exposure of Sensitive System Information to an Unauthorized Control Sphere	Vodafone H500s devices running firmware v3.5.10 (hardware model Sercomm VFH500)	https://cxsecurity.com/issue/WLB-2022010024 https://help.vodacom.co.za/personal/home/61/9493/1023659/Vodafone-H500s-WiFi-router https://www.exploit-db.com/exploits/50636 https://www.vulncheck.com/advisories/vodafone-h500s-wifi-password-disclosure-via-activation-json
https://nvd.nist.gov/vuln/detail/CVE-2025-63680	**8,6**	Nero	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Nero BackItUp in the Nero Productline is vulnerable to a path parsing/UI rendering flaw (CWE-22) that, in combination with Windows ShellExecuteW fallback extension resolution, leads to arbitrary code execution when a user clicks a crafted entry.	https://github.com/PotatoHamm/Nero-Productline-Vulnerability

https://nvd.nist.gov/vuln/detail/CVE-2025-64309	**8,6**	Brightpick Mission Control	Unprotected Transport of Credentials	Brightpick Mission Control discloses device telemetry, configuration, and credential information via WebSocket traffic to unauthenticated users when they connect to a specific URL. The unauthenticated URL can be discovered through basic network scanning techniques.	https://brightpick.ai/contact-us/ https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2025/icsa-25-317-04.json https://www.cisa.gov/news-events/ics-advisories/icsa-25-317-04
https://nvd.nist.gov/vuln/detail/CVE-2025-9317	**8,4**	Edge	Use of a Broken or Risky Cryptographic Algorithm	The vulnerability, if exploited, could allow a miscreant with read access to Edge Project files or Edge Offline Cache files to reverse engineer Edge users' app-native or Active Directory passwords through computational brute-forcing of weak hashes.	https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2025/icsa-25-317-03.json https://www.aveva.com/content/dam/aveva/documents/support/cyber-security-updates/SecurityBulletin_AVEVA-2025-006.pdf https://www.cisa.gov/news-events/ics-advisories/icsa-25-317-03
https://nvd.nist.gov/vuln/detail/CVE-2025-55034	**8,2**	Lynx+	Weak Password Requirements	General Industrial Controls Lynx+ Gateway is vulnerable to a weak password requirement vulnerability, which may allow an attacker to execute a brute-force attack resulting in unauthorized access and login.	https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2025/icsa-25-317-08.json https://www.cisa.gov/news-events/ics-advisories/icsa-25-317-08
https://nvd.nist.gov/vuln/detail/CVE-2025-59780	**7,5**	Lynx+	Missing Authentication for Critical Function	General Industrial Controls Lynx+ Gateway is missing critical authentication in the embedded web server which could allow an attacker to send GET requests to obtain sensitive device information.	https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2025/icsa-25-317-08.json https://www.cisa.gov/news-events/ics-advisories/icsa-25-317-08

https://nvd.nist.gov/vuln/detail/CVE-2025-62765	**7,5**	Lynx+	Cleartext Transmission of Sensitive Information	General Industrial Controls Lynx+ Gateway is vulnerable to a cleartext transmission vulnerability that could allow an attacker to observe network traffic to obtain sensitive information, including plaintext credentials.	https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2025/icsa-25-317-08.json https://www.cisa.gov/news-events/ics-advisories/icsa-25-317-08
https://github.com/advisories/GHSA-j4g7-v4m4-77px	**7,4**	ZITADEL	Improper Authentication	ZITADEL is vulnerable to Account Takeover with deactivated Instance IdP in github.com/zitadel/zitadel	https://github.com/golang/vulndb/blob/master/data/reports/GO-2025-4124.yaml
https://nvd.nist.gov/vuln/detail/CVE-2025-13191	**7,4**	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	A vulnerability was determined in D-Link DIR-816L 2_06_b09_beta	https://github.com/scanleale/IOT_sec/blob/main/DIR-816L%20stack%20overflow(soap.cgi).pdf https://vuldb.com/?ctiid.332480 https://vuldb.com/?id.332480 https://vuldb.com/?submit.685543 https://www.dlink.com/
https://github.com/golang/vulndb/blob/master/data/reports/GO-2025-4117.yaml	**7,2**	File Browser	Improper Authorization	File Browser is Vulnerable to Insecure Direct Object Reference (IDOR) in Share Deletion Function in github.com/filebrowser/filebrowser	https://github.com/advisories/GHSA-6cqf-cfhv-659g

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 Releases Six Industrial Control Systems Advisories	▪ ICSA-25-322-01 Schneider Electric EcoStruxure Machine SCADA Expert & Pro-face BLUE Open Studio ▪ ICSA-25-322-02 Shelly Pro 4PM ▪ ICSA-25-322-03 Shelly Pro 3EM ▪ ICSA-25-322-04 Schneider Electric PowerChute Serial Shutdown ▪ ICSA-25-322-05 METZ CONNECT EWIO2 ▪ ICSA-25-224-03 Schneider Electric EcoStruxure (Update B)	https://www.cisa.gov/news-events/alerts/2025/11/18/cisa-releases-six-industrial-control-systems-advisories
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2025-58034 Fortinet FortiWeb OS Command Code Injection Vulnerability	https://www.cisa.gov/news-events/alerts/2025/11/18/cisa-adds-one-known-exploited-vulnerability-catalog
CISA Releases Guide to Mitigate Risks from Bulletproof Hosting Providers		https://www.cisa.gov/news-events/alerts/2025/11/19/cisa-releases-guide-mitigate-risks-bulletproof-hosting-providers
CISA Adds One Known Exploited Vulnerability to Catalog	▪ CVE-2025-13223 Google Chromium V8 Type Confusion Vulnerability	https://www.cisa.gov/news-events/alerts/2025/11/19/cisa-adds-one-known-exploited-vulnerability-catalog
CISA Releases Six Industrial Control Systems Advisories	▪ ICSA-25-324-01 Automated Logic WebCTRL Premium Server ▪ ICSA-25-324-02 ICAM365 CCTV Camera Multiple Models ▪ ICSA-25-324-03 Opto 22 GRV-EPIC and GRV-RIO ▪ ICSA-25-324-04 Festo MSE6-C2M/D2M/E2M ▪ ICSA-25-324-05 Festo Didactic products ▪ ICSA-25-324-06 Emerson Appleton UPSMON-PRO	https://www.cisa.gov/news-events/alerts/2025/11/20/cisa-releases-six-industrial-control-systems-advisories

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
OpenAI Releases GPT-5.1-Codex-Max that Performs Coding Tasks Independently	https://cybersecuritynews.com/openai-releases-gpt-5-1-codex-max/
Authorities Sanctioned Russia-based Bulletproof Hosting Provider for Supporting Ransomware Operations	https://cybersecuritynews.com/bulletproof-hosting-provider-sanctioned/
pi GPT Tool Turns Your Raspberry Pi into A ChatGPT Powered AI-managed device	https://cybersecuritynews.com/pi-gpt-tool-for-raspberry-pi/
Hackers Attacking Palo Alto Networks' GlobalProtect VPN Portals with 2.3 Million Attacks	https://cybersecuritynews.com/palo-alto-vpn-under-attack/
Microsoft Investigating Copilot Issue On Processing Files	https://cybersecuritynews.com/microsoft-investigation-copilot-issue/
Microsoft Teams New Feature Let Users Report Messages Incorrectly Flagged as Security Threats	https://cybersecuritynews.com/microsoft-teams-report-messages-feature/
Microsoft Integrated Azure Firewall With AI-powered Security Copilot	https://cybersecuritynews.com/microsoft-azure-firewall-with-security-copilot/
Microsoft Threat Intelligence Briefing Agent Now Integrated With the Defender Portal	https://cybersecuritynews.com/microsoft-threat-intelligence-with-defender/
Cloudflare Discloses Technical Details Behind Massive Outage that Breaks the Internet	https://cybersecuritynews.com/cloudflare-massive-outage-details/
Google to Flag Apps on Play Store that Use Excessive Amount of battery	https://cybersecuritynews.com/google-flag-apps-on-play-store/
Cloudflare Global Outage Breaks Internet – Major Platforms on the Internet Go Down	https://cybersecuritynews.com/cloudflare-global-outage-breaks-internet/
Google Reveals Public Preview of Alert Triage and Investigation Agent for Security Operations	https://cybersecuritynews.com/google-alert-triage-investigation-agent/
Record-Breaking 15 Tbps DDoS Attack From 500,000+ Devices Hits Azure Network	https://cybersecuritynews.com/ddos-attack-azure-network/

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
Salesforce Confirms that Customers' Data Was Accessed Following the Gainsight Breach	https://cybersecuritynews.com/salesforce-gainsight-breach/
Oracle Allegedly Breached by Clop Ransomware via E-Business Suite 0-Day Hack	https://cybersecuritynews.com/oracle-breach-clop-ransomware/
WhatsApp Vulnerability Exposes 3.5 Billion Users' Phone Numbers	https://cybersecuritynews.com/whatsapp-vulnerability-exposes-3-5-billion-users/
DoorDash Confirms Data Breach – Hackers Accessed Users Personal Data	https://cybersecuritynews.com/doordash-confirms-data-breach/
Everest Ransomware Group Allegedly Exposes 343 GB of Sensitive Data in Major Under Armour Breach	https://cybersecuritynews.com/everest-ransomware-group-armour-breach/

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
SonicOS SSLVPN Vulnerability Let Attackers Crash the Firewall Remotely	https://cybersecuritynews.com/sonicos-sslvpn-vulnerability-firewall-crash/
Critical Windows Graphics Vulnerability Lets Hackers Seize Control with a Single Image	https://cybersecuritynews.com/critical-windows-graphics-vulnerability/
Threat Actors Allegedly Selling Microsoft Office 0-Day RCE Vulnerability on Hacking Forums	https://cybersecuritynews.com/microsoft-office-0-day-rce-claim/
Critical N-able N-central Vulnerabilities Allow attacker to interact with legacy APIs and read sensitive files	https://cybersecuritynews.com/critical-n-able-n-central-vulnerabilities/
Critical Twonky Server Vulnerabilities Let Attackers Bypass Authentication	https://cybersecuritynews.com/twonky-server-vulnerabilities/
Ollama Vulnerabilities Let Attackers Execute Arbitrary Code by Parsing of Malicious Model Files	https://cybersecuritynews.com/ollama-vulnerabilities-code-execution/
CISA Warns of Google Chrome 0-Day Vulnerability Exploited in Attacks	https://cybersecuritynews.com/cisa-warns-chrome-0-day-vulnerability-exploited/
Hackers Can Exploit Default ServiceNow AI Assistants Configurations to Launch Prompt Injection Attacks	https://cybersecuritynews.com/hackers-exploit-servicenow-ai-assistants/
Cline AI Coding Agent Vulnerabilities Enables Prompt Injection, Code Execution, and Data Leakage	https://cybersecuritynews.com/cline-ai-coding-agent-vulnerabilities/
Hackers Actively Exploiting 7-Zip RCE Vulnerability in the Wild	https://cybersecuritynews.com/7-zip-rce-vulnerability-exploited/

Massive Hacking Operation WrtHug Compromises Thousands of ASUS Routers Worldwide	https://cybersecuritynews.com/wrthug-asus-routers/
CISA Warns of Fortinet FortiWeb OS Command Injection Vulnerability Exploited in the Wild	https://cybersecuritynews.com/cisa-fortinet-fortiweb-vulnerability-2/
Multiple Vulnerabilities in D-Link EoL/EoS Routers Allows Remote Code Execution Attacks	https://cybersecuritynews.com/d-link-eol-eos-router-vulnerabilities/
Critical SolarWinds Serv-U Vulnerabilities Let Attackers Execute Malicious Code Remotely as Admin	https://cybersecuritynews.com/solarwinds-serv-u-vulnerabilities/
New FortiWeb 0-Day Command Injection Vulnerability Exploited in the Wild	https://cybersecuritynews.com/fortiweb-0-day-code-execution-vulnerability/
W3 Total Cache Command Injection Vulnerability Exposes 1 Million WordPress Sites to RCE Attacks	https://cybersecuritynews.com/w3-total-cache-vulnerability/
Imunify AI-Bolit Vulnerability Let Execute Arbitrary Code and Escalate Privileges to Root	https://cybersecuritynews.com/imunify-ai-bolit-vulnerability/
CISA Warns of Critical Lynx+ Gateway Vulnerability Exposes Data in Cleartext	https://cybersecuritynews.com/lynx-gateway-vulnerability/
IBM AIX Vulnerabilities Let Remote Attacker Execute Arbitrary Commands	https://cybersecuritynews.com/ibm-aix-vulnerabilities/
Chrome Type Confusion Zero-Day Vulnerability Actively Exploited in the Wild	https://cybersecuritynews.com/chrome-type-confusion-zero-day/

Patches / Updates / Fixes

Εδώ θα βρείτε τις πιο πρόσφατες διορθώσεις και ενημερώσεις ασφαλείας από προμηθευτές λογισμικού και hardware. Το περιεχόμενο αφορά συγκεκριμένα bugs ή exploits που έχουν ήδη δημοσιοποιηθεί, μαζί με οδηγίες για το πώς να εφαρμοστούν τα patches.

Σύντομη περιγραφή / Τίτλος	URL

Potential threats / Threat intelligence

Η συγκεκριμένη ενότητα ασχολείται με νέες απειλές, εξελιγμένα malware και τεχνικές επιθέσεων που έχουν εντοπιστεί σε πραγματικές συν-θήκες. Περι-λαμβάνονται αναφορές σε εργαλεία που χρησιμοποιούν οι επιτιθέμενοι, αλλά και δείκτες (IoCs) που μπορούν να χρησιμοποιηθούν στην άμυνα.

Σύντομη περιγραφή / Τίτλος	URL
Tsundere Botnet Abusing Popular Node.js and Cryptocurrency Packages to Attack Windows, Linux, and macOS Users	https://cybersecuritynews.com/tsundere-botnet-abusing-popular-node-js-and-cryptocurrency-packages/
Sturnus Banking Malware Steals Communications from Signal and WhatsApp, Gaining Full Control of The Device	https://cybersecuritynews.com/sturnus-banking-malware-steals-communications-from-signal-and-whatsapp/
Samourai Wallet Cryptocurrency Mixing Founders Jailed for Laundering Over $237 Million	https://cybersecuritynews.com/samourai-wallet-cryptocurrency-mixing-founders-jailed/
New Ransomware Variants Targeting Amazon S3 Services Leveraging Misconfigurations and Access Controls	https://cybersecuritynews.com/new-ransomware-variants-targeting-amazon-s3-services/
TamperedChef Hacking Campaign Leverages Common Apps to Deliver Payloads and Gain Remote Access	https://cybersecuritynews.com/tamperedchef-hacking-campaign-leverages-common-apps/
Lessons from Oracle E-Business Suite Hack That Allegedly Compromises Nearly 30 Organizations Worldwide	https://cybersecuritynews.com/oracle-e-business-suite-hack/
New Malware Via WhatsApp Exfiltrate Contacts to Attack Server and Deploys Malware	https://cybersecuritynews.com/new-malware-via-whatsapp-exfiltrate-contacts/
GenAI Makes it Easier for Cybercriminals to Successfully Lure Victims into Scams	https://cybersecuritynews.com/genai-makes-it-easier-for-cybercriminals/
Threat Actors Pioneering a New Operational Model That Combines Digital and Physical Threats	https://cybersecuritynews.com/threat-actors-pioneering-a-new-operational-model/
Researchers Disclosed Analysis of Rhadamanthys Loader's Anti-Sandboxing and Anti-AV Emulation Features	https://cybersecuritynews.com/researchers-disclosed-analysis-of-rhadamanthys-loaders-anti-sandboxing/
China-Nexus APT Group Leverages DLL Sideloading Technique to Attack Government and Media Sectors	https://cybersecuritynews.com/china-nexus-apt-group-leverages-dll-sideloading-technique/
'The Gentlemen' Ransomware Group with Dual-Extortion Strategy Encrypts and Exfiltrates Data	https://cybersecuritynews.com/the-gentlemen-ransomware-group/
Chinese PlushDaemon Hackers use EdgeStepper Tool to Hijack Legitimate Updates and Redirect to Malicious Servers	https://cybersecuritynews.com/chinese-plushdaemon-hackers-use-edgestepper-tool/
Hackers Using Leverage Tuoni C2 Framework Tool to Stealthily Deliver In-Memory Payloads	https://cybersecuritynews.com/hackers-using-leverage-tuoni-c2-framework-tool/
Destructive Akira Ransomware Attack with a Single Click on CAPTCHA in Malicious Website	https://cybersecuritynews.com/destructive-akira-ransomware-attack/
New Nova Stealer Attacking macOS Users by Swapping Legitimate Apps to Steal Cryptocurrency Wallet Data	https://cybersecuritynews.com/new-nova-stealer-attacking-macos-users/
New ShadowRay Attack Exploit Ray AI-Framework Vulnerability to Attack AI Systems	https://cybersecuritynews.com/new-shadowray-attack-exploit-ray-ai-framework/
New npm Malware Campaign Verifies if the Visitor is a Victim or a Researcher Before Triggering Infection	https://cybersecuritynews.com/new-npm-malware-campaign/
New .NET Malware Hides Lokibot Malware within PNG/BMP Files to Evade Detection	https://cybersecuritynews.com/new-net-malware-hides-lokibot-malware/

New Sneaky 2FA Phishing Kit with BitB Technique Attacking Users to Steal Microsoft Account Credentials	https://cybersecuritynews.com/new-sneaky-2fa-phishing-kit-with-bitb-technique-attacking-users/
Malicious 'Free' VPN Extension with 9 Million Installs Hijacks User Traffic and Steals Browsing Data	https://cybersecuritynews.com/malicious-free-vpn-extension-with-9-million-installs/
Eurofiber Data Breach – Hackers Exploited Vulnerability to Exfiltrate Users' Data	https://cybersecuritynews.com/eurofiber-data-breach/
Princeton University Data Breach – Database with Donor Info Compromised	https://cybersecuritynews.com/princeton-university-data-breach/
WhatsApp Screen-Sharing Scam Let Attackers Trick Users into Revealing Sensitive Data	https://cybersecuritynews.com/whatsapp-screen-sharing-scam/
Authorities Seized Thousands of Servers from Rogue Hosting Company Used to Fuel Cyberattacks	https://cybersecuritynews.com/authorities-seized-thousands-of-servers/
Remcos RAT C2 Activity Mapped Along with The Ports Used for Communications	https://cybersecuritynews.com/remcos-rat-c2-activity-mapped/
Lazarus APT Group New ScoringMathTea RAT Enables Remote Command Execution Among Other Capabilities	https://cybersecuritynews.com/lazarus-apt-group-new-scoringmathtea-rat/
UNC1549 Hackers with Custom Tools Attacking Aerospace and Defense Systems to Steal Logins	https://cybersecuritynews.com/unc1549-hackers-with-custom-tools/
Threat Actors Leveraging Compromised RDP Logins to Deploy Lynx Ransomware After Deleting Server Backups	https://cybersecuritynews.com/threat-actors-leveraging-compromised-rdp-logins-to-deploy-lynx/

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
NSA Issues Guidance for ISPs and Network Defenders to Combat Malicious Activity	https://cybersecuritynews.com/nsa-release-guidance-bulletproof-hosting/
How to Solve Alert Overload in Your SOC	https://cybersecuritynews.com/how-to-solve-alert-overload-in-your-soc/
Sysmon – Go-to Tool for IT Admins, Security Pros, and Threat Hunters Coming to Windows	https://cybersecuritynews.com/sysmon-tool-windows/

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/