CVEs

URL ευπάθειας (NIST NVD)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	Συσκευές/Εκδόσεις που ΔΕΝ επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2024-47875	10	DOMPurify (DOM-only, super-fast, uber-tolerant XSS sanitizer for HTML, MathML and SVG)	nesting-based mXSS	N/A	fixed in 2.5.0 and 3.1.3	https://github.com/cure53/DOMPurify https://github.com/cure53/DOMPurify/security/advisories/GHSA-gx9m-whjm-85jf
https://nvd.nist.gov/vuln/detail/CVE-2024-9985	10	Enterprise Cloud Database from Ragic	Unrestricted Upload of File with Dangerous Type	N/A	N/A	https://www.ragic.com/ https://www.twcert.org.tw/en/cp-139-8153-1120e-2.html https://www.twcert.org.tw/tw/cp-132-8152-09e81-1.html
https://nvd.nist.gov/vuln/detail/CVE-2024-9047	9.8	WordPress File Upload plugin for WordPress	Path Traversal	all versions up to, and including, 4.24.11	N/A	https://wordpress.org/plugins/wp-file-upload/ https://www.wordfence.com/threat-intel/vulnerabilities/id/554a314c-9e8e-4691-9792-d086790ef40f?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-9707	9.8	Hunk Companion plugin for WordPress	Missing Authorization	all versions up to, and including, 1.8.4	N/A	https://wordpress.org/plugins/hunk-companion/ https://www.wordfence.com/threat-intel/vulnerabilities/id/9c101fca-037c-4bed-9dc7-baa021a8b59c?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-45275	9.8	mbNET.mini router	Use of Hard-coded Credentials	N/A	N/A	https://mbconnectline.com/mbnet-mini-en/ https://cert.vde.com/en/advisories/VDE-2024-056
https://nvd.nist.gov/vuln/detail/CVE-2024-9925	9.8	TAI Smart Factory's QPLANT SF	SQL Injection	N/A	N/A	https://www.taismartfactory.com/en/qplant-sf/ https://incibe.es/en/incibe-cert/notices/aviso-sci/sql-injection-qplant-tai-smart-factory
https://nvd.nist.gov/vuln/detail/CVE-2024-9164 https://nvd.nist.gov/vuln/detail/CVE-2024-8970	9.6	GitLab CE/EE	Missing Authentication for Critical Function Incorrect Authorization	Multiple versions (please check the provided links)	N/A	https://about.gitlab.com/install/ce-or-ee/ https://gitlab.com/gitlab-org/gitlab/-/issues/493946 https://gitlab.com/gitlab-org/gitlab/-/issues/490916
https://nvd.nist.gov/vuln/detail/CVE-2024-9137	9.4	Moxa products	Missing Authentication for Critical Function	N/A	N/A	https://www.moxa.com/en https://www.moxa.com/en/support/product-support/security-advisory/mpsa-241154-missing-authentication-and-os-command-injection-vulnerabilities-in-routers-and-network-security-appliances
https://nvd.nist.gov/vuln/detail/CVE-2024-45733 https://nvd.nist.gov/vuln/detail/CVE-2024-45732 https://nvd.nist.gov/vuln/detail/CVE-2024-45731	8.8	Splunk Enterprise for Windows	Deserialization of Untrusted Data	multiple versions and products	N/A	https://www.splunk.com/en_us/products/splunk-enterprise.html https://advisory.splunk.com/advisories/SVD-2024-1003 https://advisory.splunk.com/advisories/SVD-2024-1002 https://advisory.splunk.com/advisories/SVD-2024-1001
https://nvd.nist.gov/vuln/detail/CVE-2024-9915	8.8	D-Link DIR-619L	Classic Buffer Overflow	B1 2.06	N/A	https://www.dlink.com.sg/product/dir-619l-n300-high-power-wireless-router-2/ https://github.com/abcdefg-png/IoT-vulnerable/blob/main/D-Link/DIR-619L/formVirtualServ.md
https://nvd.nist.gov/vuln/detail/CVE-2024-8070	8.5	Schneider Electric	Cleartext Storage of Sensitive Information	N/A	N/A	https://www.se.com/ww/en/ https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-282-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-282-04.pdf

https://nvd.nist.gov/vuln/detail/CVE-2024-48020	8.5	Revmakx Backup and Staging by WP Time Capsule	SQL Injection	from n/a through 1.22.21	N/A	https://wordpress.org/plugins/wp-time-capsule/ https://patchstack.com/database/vulnerability/wp-time-capsule/wordpress-backup-and-staging-by-wp-time-capsule-plugin-1-22-21-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-35520https://nvd.nist.gov/vuln/detail/CVE-2024-35519	8.4	Netgear products	Command Injection	R7000 1.0.11.136EX6120 v1.0.0.68, Netgear EX6100 v1.0.2.28, and Netgear EX3700 v1.0.0.96	N/A	https://www.netgear.com/home/wifi/routers/r7000/https://www.netgear.com/support/product/ex6120/https://kb.netgear.com/000066027/Security-Advisory-for-Post-Authentication-Command-Injection-on-the-R7000-PSV-2023-0154https://github.com/consrc/cves/blob/main/CVE-2024-35519.md
https://nvd.nist.gov/vuln/detail/CVE-2024-35522 https://nvd.nist.gov/vuln/detail/CVE-2024-35517	8.4	Netgear EX3700 Netgear XR1000	command injection	before 1.0.0.98 v1.0.0.64	N/A	https://www.netgear.com/home/wifi/range-extenders/ex3700/ https://www.netgear.com/home/online-gaming/routers/xr1000/ https://github.com/consrc/cves/blob/main/CVE-2024-35522.md https://github.com/consrc/cves/blob/main/CVE-2024-35517.md
https://nvd.nist.gov/vuln/detail/CVE-2024-8755	8.4	Progress LoadMaster	Improper Input Validation	Multiple versions	N/A	https://kemptechnologies.com/kemp-load-balancers https://support.kemptechnologies.com/hc/en-us/articles/30297374715661-LoadMaster-Security-Vulnerability-CVE-2024-8755
https://nvd.nist.gov/vuln/detail/CVE-2024-47504 https://nvd.nist.gov/vuln/detail/CVE-2024-47502 https://nvd.nist.gov/vuln/detail/CVE-2024-47499 https://nvd.nist.gov/vuln/detail/CVE-2024-47497 https://nvd.nist.gov/vuln/detail/CVE-2024-47491 https://nvd.nist.gov/vuln/detail/CVE-2024-47490 https://nvd.nist.gov/vuln/detail/CVE-2024-39563 https://nvd.nist.gov/vuln/detail/CVE-2024-39547	8.2	Juniper Networks Junos OS	Multiple vulnerabilities	multiple versions and products	N/A	https://www.juniper.net/content/dam/www/assets/datasheets/us/en/security/srx5400-srx5600-srx5800-firewall-datasheet.pdf https://www.juniper.net/ https://supportportal.juniper.net/JSA88134 https://supportportal.juniper.net/JSA88132 https://supportportal.juniper.net/JSA88129 https://supportportal.juniper.net/ https://supportportal.juniper.net/JSA83009 https://supportportal.juniper.net/JSA88110 https://supportportal.juniper.net/JSA88108
https://nvd.nist.gov/vuln/detail/CVE-2024-33581 https://nvd.nist.gov/vuln/detail/CVE-2024-33580 https://nvd.nist.gov/vuln/detail/CVE-2024-33579 https://nvd.nist.gov/vuln/detail/CVE-2024-33578	7.8	Lenovo (Software products)	Uncontrolled Search Path Element	Lenovo PC Manager Lenovo Personal Cloud Lenovo Baiying Lenovo Leyun	N/A	https://www.lenovo.com/gr/el/ https://iknow.lenovo.com.cn/detail/423563
https://nvd.nist.gov/vuln/detail/CVE-2024-45316	7.8	SonicWall Connect Tunnel	Improper Link Resolution	version 12.4.3.271 and earlier of Windows client	N/A	https://www.sonicwall.com/products/remote-access/vpn-clients https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0017
https://nvd.nist.gov/vuln/detail/CVE-2024-9548	7.2	SlimStat Analytics plugin for WordPress	Cross-site Scripting	all versions up to, and including, 5.2.6	N/A	https://wordpress.org/plugins/wp-slimstat/ https://www.wordfence.com/threat-intel/vulnerabilities/id/fa91912d-5794-4c96-8a13-bd54ce0f1deb?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-8531	7.2	Data Center Expert software	Improper Verification of Cryptographic Signature	N/A	N/A	https://www.se.com/us/en/product-range/61851-ecostruxure-it-data-center-expert/#products https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-282-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-282-01.pdf

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Releases Industrial Control Systems Advisories	ICSA-24-289-01 Siemens Siveillance Video Camera ICSA-24-289-02 Schneider Electric Data Center Expert	https://www.cisa.gov/news-events/alerts/2024/10/15/cisa-releases-two-industrial-control-systems-advisories
CISA Adds Known Exploited Vulnerabilities to Catalog	CVE-2024-30088 Microsoft Windows Kernel TOCTOU Race Condition Vulnerability CVE-2024-9680 Mozilla Firefox Use-After-Free Vulnerability CVE-2024-28987 SolarWinds Web Help Desk Hardcoded Credential Vulnerability	https://www.cisa.gov/news-events/alerts/2024/10/15/cisa-adds-three-known-exploited-vulnerabilities-catalog

News

Σύντομη περιγραφή / Τίτλος	URL
UK: NCSC Offers Education Organizations Free Cyber Services	https://www.infosecurity-magazine.com/news/uk-ncsc-education-free-cyber/
TrickMo Banking Trojan Can Now Capture Android PINs and Unlock Patterns	https://thehackernews.com/2024/10/trickmo-banking-trojan-can-now-capture.html
New Telekopye Scam Toolkit Targeting Booking.com and Airbnb Users	https://hackread.com/telekopye-scam-toolkit-hit-booking-com-airbnb-users/
LLMs Are a New Type of Insider Adversary	https://www.darkreading.com/vulnerabilities-threats/llms-are-new-type-insider-adversary
Most Organizations Unprepared for Post-Quantum Threat	https://www.infosecurity-magazine.com/news/orgs-unprepared-postquantum-threat/
Microsoft: Schools Grapple With Thousands of Cyberattacks Weekly	https://www.darkreading.com/cybersecurity-operations/microsoft-k-12-universities-grapple-with-thousands-attacks-weekly
U.S. CISA adds Fortinet products and Ivanti CSA bugs to its Known Exploited Vulnerabilities catalog	https://securityaffairs.com/169804/security/u-s-cisa-adds-fortinet-products-and-ivanti-csa-bugs-known-exploited-vulnerabilities-catalog.html
CISA Urges Encryption of Cookies in F5 BIG-IP Systems	https://www.infosecurity-magazine.com/news/cisa-urges-encryption-cookies-f/
Zero-day Flaws Exposed EV Chargers to Shutdowns and Data Theft	https://hackread.com/zero-day-flaws-ev-chargers-to-shutdowns-data-theft/

News - Breaches

Σύντομη περιγραφή / Τίτλος	URL
Separate health breaches impact over 500K	https://www.scworld.com/brief/separate-health-breaches-impact-over-500k
Data breaches trigger increase in cyber insurance claims	https://www.helpnetsecurity.com/2024/10/15/cyber-claims-frequency/
Cisco investigates breach after stolen data for sale on hacking forum	https://www.bleepingcomputer.com/news/security/cisco-investigates-breach-after-stolen-data-for-sale-on-hacking-forum/
Casio Confirms Ransomware Outage and Data Breach	https://www.infosecurity-magazine.com/news/casio-confirms-ransomware-outage/

News – Vulnerabilities and Flaws

Σύντομη περιγραφή / Τίτλος	URL
Jetpack patches critical bug that exposed data on 27M WordPress sites	https://www.scworld.com/news/jetpack-patches-critical-bug-that-exposed-data-on-27m-wordpress-sites
WP Engine Accuses WordPress of 'Forcibly' Taking Over Its Plug-in	https://www.darkreading.com/application-security/wp-engine-accuses-wordpress-forcibily-taking-over-plug-in
87,000+ Fortinet devices still open to attack, are yours among them? (CVE-2024-23113)	https://www.helpnetsecurity.com/2024/10/15/cve-2024-23113/
Serious Adversaries Circle Ivanti CSA Zero-Day Flaws	https://www.darkreading.com/cyberattacks-data-breaches/serious-adversaries-circle-ivanti-csa-flaws
Vulnerable instances of Log4j still being used nearly 3 years later	https://www.scworld.com/news/vulnerable-instances-of-log4j-still-being-used-nearly-3-years-later
Critical Veeam Vulnerability Exploited to Spread Akira and Fog Ransomware	https://thehackernews.com/2024/10/critical-veeam-vulnerability-exploited.html
Juniper Networks Patches Dozens of Vulnerabilities	https://www.securityweek.com/juniper-networks-patches-dozens-of-vulnerabilities/

News – Potential Threats / Threat Intelligence

Σύντομη περιγραφή / Τίτλος	URL
EDRSilencer red team tool used in attacks to bypass security	https://www.bleepingcomputer.com/news/security/edrsilencer-red-team-tool-used-in-attacks-to-bypass-security/
A new Linux variant of FASTCash malware targets financial systems	https://securityaffairs.com/169860/malware/new-linux-variant-fastcash-malware-targets-financial-systems.html
Android PINs exfiltrated by newly emergent TrickMo malware variants	https://www.scworld.com/brief/android-pins-exfiltrated-by-newly-emergent-trickmo-malware-variants
Ivanti CSA bugs leveraged in suspected nation-state attack	https://www.scworld.com/brief/ivanti-csa-bugs-leveraged-in-suspected-nation-state-attack
New Malware Campaign Uses PureCrypter Loader to Deliver DarkVision RAT	https://thehackernews.com/2024/10/new-malware-campaign-uses-purecrypter.html
Cerberus Android Banking Trojan Deployed in New Multi-Stage Malicious Campaign	https://www.infosecurity-magazine.com/news/cerberus-android-banking-trojan/
High-severity Windows vulnerability leveraged in new OilRig APT attacks	https://www.scworld.com/brief/high-severity-windows-vulnerability-leveraged-in-new-oilrig-apt-attacks

News – Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
How open source SIEM and XDR tackle evolving threats	https://www.bleepingcomputer.com/news/security/how-open-source-siem-and-xdr-tackle-evolving-threats/
SIEM for Small and Medium-Sized Enterprises: What you need to know	https://securityaffairs.com/168584/security/siem-sbms-enterprises.html