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-2023-7028	**10**	GitLab CE/EE	reset emails could be delivered to an unverified email address	all versions from 16.1 prior to 16.1.6, 16.2 prior to 16.2.9, 16.3 prior to 16.3.7, 16.4 prior to 16.4.5, 16.5 prior to 16.5.6, 16.6 prior to 16.6.4, and 16.7 prior to 16.7.2	N/A	https://about.gitlab.com/install/ce-or-ee/ https://gitlab.com/gitlab-org/gitlab/-/issues/436084
https://nvd.nist.gov/vuln/detail/CVE-2024-41110	**9.9**	Moby is an open-source project created by Docker	Partial String Comparison	N/A	19.0, 20.0, 23.0, 24.0, 25.0, 26.0,	https://github.com/moby/moby https://github.com/moby/moby/security/advisories/GHSA-v23v-6jw2-98fq

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**
		for software containerization			and 26.1	
https://nvd.nist.gov/vuln/detail/CVE-2023-45249	**9.8**	Acronis Cyber Infrastructure	Remote command execution	before build 5.0.1-61, before build 5.1.1-71, before build 5.2.1-69, before build 5.3.1-53, before build 5.4.4-132	N/A	https://www.acronis.com/en-us/support/providers/aci/ https://security-advisory.acronis.com/advisories/SEC-6452
https://nvd.nist.gov/vuln/detail/CVE-2024-37084	**9.8**	Spring Cloud Data Flow	Path Traversal	prior to 2.11.4	N/A	https://spring.io/projects/spring-cloud-dataflow https://spring.io/security/cve-2024-37084
https://nvd.nist.gov/vuln/detail/CVE-2024-41461	**9.8**	Tenda FH1201	Out-of-bounds Write	v1.2.0.14	N/A	https://www.tendacn.com/download/detail-3322.html https://github.com/iotresearch/iot-vuln/blob/main/Tenda/FH1201/DhcpListClient/READ

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**
						ME.md
https://nvd.nist.gov/vuln/detail/CVE-2024-6327	**9.8**	Progress® Telerik® Report Server	Deserialization of Untrusted Data	versions prior to 2024 Q2 (10.1.24.709)	N/A	https://www.telerik.com/report-server https://docs.telerik.com/report-server/knowledge-base/deserialization-vulnerability-cve-2024-6327
https://nvd.nist.gov/vuln/detail/CVE-2022-46836	**9.1**	Checkmk	PHP code injection	<= 2.1.0p10, <= 2.0.0p27, and <= 1.6.0p29	N/A	https://checkmk.com/ https://checkmk.com/werk/14383
https://nvd.nist.gov/vuln/detail/CVE-2024-41914	**9**	EdgeConnect SD-WAN Orchestrator	Cross-site Scripting	N/A	N/A	https://www.arubanetworks.com/products/sd-wan/edgeconnect/orchestrator/ https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04672en_us&docLocale=en_US

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-2018-7311	**8.8**	PrivateVPN	root privilege escalation	2.0.31	N/A	https://privatevpn.com/ https://github.com/VerSprite/research/blob/master/advisories/VS-2018-004.md
https://nvd.nist.gov/vuln/detail/CVE-2024-4845	**8.8**	Icegram Express plugin for WordPress	SQL Injection	all versions up to, and including, 5.7.22	N/A	https://wordpress.org/plugins/email-subscribers/ https://www.wordfence.com/threat-intel/vulnerabilities/id/21be2215-8ce0-438e-94e0-6a350b8cc952?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-41136	**8.8**	HPE Aruba Networking EdgeConnect SD-WAN gateways	OS Command Injection	N/A	N/A	https://buy.hpe.com/us/en/as-a-service/private-hybrid-cloud-saas/aruba-connectivity-saas/aruba-connectivity/hpe-aruba-networking-edgeconnect-sd-wan/p/1014658646 https://csaf.arubanetworks.com/2024/hpe_aruba_networking_-_hpesbnw04673.txt
https://nvd.nist.gov/vuln/detail/CVE-2024-31970	**8.8**	AdTran SRG 834-5 HDC17600021F1	gain unauthorized root access	HDC17600021F1 devices (with SmartOS	SmartOS Version 12.1.3.1	https://www.adtran.com/en/products-and-services/residential-solutions/mesh-wi-fi-gateways-and-satellites/service-delivery-gateways https://github.com/actuator/cve/blob/main/AdTran/CV

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**
				11.1.1.1)		E-2024-31970
https://nvd.nist.gov/vuln/detail/CVE-2024-40872	**8.4**	Absolute Secure Access	Untrusted Pointer Dereference	prior to version 13.07	N/A	https://www.absolute.com/platform/secure-access/ https://www.absolute.com/platform/security-information/vulnerability-archive/secure-access-1307/cve-2024-40872/
https://nvd.nist.gov/vuln/detail/CVE-2024-38872	**8.3**	Zohocorp ManageEngine Exchange Reporter Plus	SQL Injection	versions 5717 and below	N/A	https://store.manageengine.com/exchange-reports/ https://www.manageengine.com/products/exchange-reports/advisory/CVE-2024-38872.html
https://nvd.nist.gov/vuln/detail/CVE-2022-48851	**7.8**	GDM (Linux kernel)	use after free	N/A	N/A	https://wiki.archlinux.org/title/GDM https://git.kernel.org/stable/c/fc7f750dc9d102c1ed7bbe4591f991e770c99033
https://nvd.nist.gov/vuln/detail/CVE-2024-4467	**7.8**	QEMU disk image utility (qemu-img) 'info' command	denial of service or read/write to an existing	N/A	N/A	https://qemu-project.gitlab.io/qemu/tools/qemu-img.html https://access.redhat.com/security/cve/CVE-2024-4467

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**
			external file			
https://nvd.nist.gov/vuln/detail/CVE-2024-39894	**7.5**	OpenSSH	allows timing attacks	9.5 through 9.7 before 9.8	N/A	https://www.openssh.com/ https://www.openssh.com/txt/release-9.8
https://nvd.nist.gov/vuln/detail/CVE-2024-38512	**7.2**	Lenovo XClarity Controller (XCC)	command injection	N/A	N/A	https://pubs.lenovo.com/xcc/dw1lm_c_ch1_introduction https://support.lenovo.com/us/en/product_security/LEN-156781

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	**Αναγνωριστικό ευπάθειας**	**URL**
Widespread IT Outage Due to CrowdStrike Update	CrowdStrike Update	https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update
Infrastructure Resilience Planning Framework (IRPF) Playbook		https://www.cisa.gov/resources-tools/resources/infrastructure-resilience-planning-framework-irpf-playbook
CISA Releases Four Industrial Control Systems Advisories	ICSA-24-205-01 National Instruments IO Trace ICSA-24-205-02 Hitachi Energy AFS/AFR Series Products ICSA-24-205-03 National Instruments LabVIEW ICSA-22-333-02 Hitachi Energy IED Connectivity Packages and PCM600 Products (Update A) ICSA-24-207-01 Siemens SICAM Products ICSA-24-207-02 Positron Broadcast Signal Processor	https://www.cisa.gov/news-events/alerts/2024/07/23/cisa-releases-four-industrial-control-systems-advisories https://www.cisa.gov/news-events/alerts/2024/07/25/cisa-releases-two-industrial-control-systems-advisories
CISA Adds Two Known Exploited Vulnerabilities to Catalog	CVE-2012-4792 Microsoft Internet Explorer Use-After-Free Vulnerability CVE-2024-39891 Twilio Authy Information Disclosure Vulnerability	https://www.cisa.gov/news-events/alerts/2024/07/23/cisa-adds-two-known-exploited-vulnerabilities-catalog

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	**Αναγνωριστικό ευπάθειας**	**URL**
ISC Releases Security Advisories for BIND 9	CVE-2024-4076: Assertion failure when serving both stale cache data and authoritative zone content CVE-2024-1975: SIG(0) can be used to exhaust CPU resources CVE-2024-1737: BIND's database will be slow if a very large number of RRs exist at the same name CVE-2024-0760: A flood of DNS messages over TCP may make the server unstable	https://www.cisa.gov/news-events/alerts/2024/07/24/isc-releases-security-advisories-bind-9