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-2023-41918	**10**	P1/P2 4G Cellular Bonding Video Encoder	Missing Authentication for Critical Function	N/A	N/A	https://www.kiloview.com/en/encoder/4g-bonding-encoder/ https://advisories.ncsc.nl/advisory?id=NCSC-2024-0273
https://nvd.nist.gov/vuln/detail/CVE-2024-38366	**10**	trunk.cocoapods.org is the authentication server for the CoacoaPods	Injection	N/A	patched server-side with commit 001cc3a430e75a16307f5fd6cdff1363ad2f40f3 in September 2023	https://github.com/CocoaPods/trunk.cocoapods.org https://github.com/CocoaPods/CocoaPods/security/advisories/GHSA-x2x4-g675-qg7c
https://nvd.nist.gov/vuln/detail/CVE-2024-37112	**10**	Membership Software WishList Member X	SQL Injection	from n/a before 3.26.7	N/A	https://wishlistmember.com/ https://patchstack.com/database/vulnerability/wishlist-member-x/wordpress-wishlist-member-x-plugin-3-25-1-unauthenticated-arbitrary-

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**
						sql-query-execution-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-39943	**9.9**	rejetto HFS (aka HTTP File Server)	OS command execution by remote authenticated users	N/A	N/A	https://www.rejetto.com/hfs/ https://github.com/rejetto/hfs/commit/305381bd36eee074fb238b64302a252668daad1d https://github.com/rejetto/hfs/compare/v0.52.9...v0.52.10 https://www.rejetto.com/wiki/index.php/HFS:_Working_with_uploads
https://nvd.nist.gov/vuln/detail/CVE-2024-39931	**9.9**	Gogs (A painless self-hosted Git service.)	allows deletion of internal files	through 0.13.0	N/A	https://gogs.io/ https://github.com/gogs/gogs/releases https://www.sonarsource.com/blog/securing-

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**
						developer-tools-unpatched-code-vulnerabilities-in-gogs-1/
https://nvd.nist.gov/vuln/detail/CVE-2024-3604	**9.9**	OSM – OpenStreetMap plugin for WordPress	SQL Injection	all versions up to, and including, 6.0.2	N/A	https://wordpress.org/plugins/osm/ https://www.wordfence.com/threat-intel/vulnerabilities/id/c8eebc67-e590-4d7f-8925-e5e5090cedf0?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-37185	**9.8**	OpenHarmony	Out-of-bounds Write	v4.0.0	N/A	https://gitee.com/openharmony/docs/blob/master/en/OpenHarmony-Overview.md https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2024/2024-

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**
						07.md
https://nvd.nist.gov/vuln/detail/CVE-2024-6172	**9.8**	Email Subscribers by Icegram Express – Email Marketing, Newsletters, Automation for WordPress & WooCommerce plugin for WordPress	SQL Injection	all versions up to, and including, 5.7.25	N/A	https://wordpress.org/plugins/email-subscribers/ https://www.wordfence.com/threat-intel/vulnerabilities/id/13629598-d45d-4ff5-aeb5-6ac881d25183?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-39309	**9.8**	Parse Server (open source backend)	Authentication Bypass Using an Alternate Path or Channel	versions prior to 6.5.7 and 7.1.0	N/A	https://parseplatform.org/ https://github.com/parse-community/parse-server/security/advisories/GHSA-c2hr-cqg6-8j6r
https://nvd.nist.gov/vuln/detail/CVE-2024-28747	**9.8**	SmartSPS devices	Use of Hard-coded Credentials	N/A	N/A	https://supplyline.com/product/ifm/050/050015/050015010/ https://cert.vde.com/en/ad

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**
						visories/VDE-2024-012
https://nvd.nist.gov/vuln/detail/CVE-2023-46685	**9.8**	LevelOne WBR-6013	Use of Hard-coded Password	RER4_A_v3411b_2T2R_LEV_09_170623	N/A	https://us.level1.com/de-de/products/wbr-6013 https://talosintelligence.com/vulnerability_reports/TALOS-2023-1871
https://nvd.nist.gov/vuln/detail/CVE-2024-27903	**9.8**	OpenVPN plug-ins on Windows	Unverified Ownership	2.6.9	N/A	https://openvpn.net/ https://www.tenable.com/cve/CVE-2024-27903 https://community.openvpn.net/openvpn/wiki/CVE-2024-27903 https://openvpn.net/security-advisory/ovpnx-vulnerability-cve-2024-27903-cve-2024-27459-cve-2024-24974/ https://www.mail-archive.com/openvpn-

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**
						users@lists.sourceforge.net/msg07534.html
https://nvd.nist.gov/vuln/detail/CVE-2024-4708	**9.3**	mySCADA myPRO	Use of Hard-coded Password	N/A	N/A	https://www.myscada.org/mypro/ https://www.cisa.gov/news-events/ics-advisories/icsa-24-184-02 https://www.myscada.org/mypro/
https://nvd.nist.gov/vuln/detail/CVE-2024-5322	**9.1**	N-central server	Authentication Bypass Using an Alternate Path or Channel	prior to 2024.3	N/A	https://documentation.n-able.com/N-central/userguide/Content/ReleaseDocs/Install_Config/InstallConfig_InstallOverview.htm https://me.n-able.com/s/security-advisory/aArVy0000000B

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**
						gDKAU/cve20245322-ncentral-authentication-bypass-via-session-rebinding
https://nvd.nist.gov/vuln/detail/CVE-2024-37555	**9.1**	ZealousWeb Generate PDF using Contact Form 7.	Unrestricted Upload of File with Dangerous Type	from n/a through 4.0.6	N/A	https://wordpress.org/support/plugin/generate-pdf-using-contact-form-7/ https://patchstack.com/database/vulnerability/generate-pdf-using-contact-form-7/wordpress-generate-pdf-using-contact-form-7-plugin-4-0-6-arbitrary-file-upload-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-28751	**9.1**	Vulnerabilities in ifm AC14 firmware	OS Command Injection	N/A	N/A	https://www.ifm.com/de/en/download/eco300_SmartSPS_AC14_AC4S_Firmware https://cert.vde.com/en/ad

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**
						visories/VDE-2024-012
https://nvd.nist.gov/vuln/detail/CVE-2024-37082	**9**	HAProxy	Authentication Bypass by Spoofing	prior to v40.17.0	N/A	https://www.haproxy.org/ https://www.cloudfoundry.org/blog/cve-2024-37082-mtls-bypass/
https://nvd.nist.gov/vuln/detail/CVE-2024-5943	**8.8**	Nested Pages plugin for WordPress	Cross-Site Request Forgery (CSRF)	all versions up to, and including, 3.2.7	N/A	https://wordpress.org/plugins/wp-nested-pages/ https://www.wordfence.com/threat-intel/vulnerabilities/id/c2663150-61f9-49e3-9219-fbe89cc6b03c?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-3904	**8.8**	MELIPC Series MI5122-VW (Smart Device Communication Gateway)	Incorrect Default Permissions	versions "05" to "07"	N/A	https://mitsubishi-electric-eshop.mee.com/mee/FA_IA/en/EUR/Catalogue/PLC/PLC-Modular/CPU-Module/MI5122-

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**
						VW/p/000000000000337054 https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2024-003_en.pdf
https://nvd.nist.gov/vuln/detail/CVE-2024-2385	**8.8**	Elementor Addons by Livemesh plugin for WordPress	Local File Inclusion	all versions up to, and including, 8.3.7	N/A	https://wordpress.org/plugins/addons-for-elementor/ https://www.wordfence.com/threat-intel/vulnerabilities/id/0aa3ec9b-80d5-4e31-8045-43c8d151cab8?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-36985	**8.8**	Splunk Enterprise versions	Function Call With Incorrectly Specified Argument	versions below 9.2.2, 9.1.5, and 9.0.10	N/A	https://www.splunk.com/?301=/en_us https://advisory.splunk.com/advisories/SVD-2024-

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**
			Value			0705
https://nvd.nist.gov/vuln/detail/CVE-2024-6166	**8.8**	Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress	time-based SQL Injection	all versions up to, and including, 1.5.112	N/A	https://wordpress.org/plugins/unlimited-elements-for-elementor/ https://www.wordfence.com/threat-intel/vulnerabilities/id/9826c91c-0f6e-4d3b-bc14-4af6b60ef246?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2023-47677	**8.8**	Realtek rtl819x Jungle SDK	Cross-Site Request Forgery (CSRF)	v3.4.12	N/A	https://www.realtek.com/ https://www.talosintelligence.com/vulnerability_reports/TALOS-2023-1895
https://nvd.nist.gov/vuln/detail/CVE-2024-39937	**8.6**	supOS 5.0 (Industrial Operating System)	directory traversal	5	N/A	https://www.supos.ai/ https://github.com/bytehunter-rat/supOS-BUG/blob/main/supOSDi

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**
						rectoryTraversal.md https://www.supos.com/supOSindex
https://nvd.nist.gov/vuln/detail/CVE-2024-34361	**8.5**	Pi-hole is a DNS sinkhole	Server-Side Request Forgery (SSRF)	versions prior to 5.18.3	N/A	https://pi-hole.net/ https://github.com/pi-hole/pi-hole/security/advisories/GHSA-jg6g-rrj6-xfg6
https://nvd.nist.gov/vuln/detail/CVE-2024-39742	**8.1**	IBM MQ Operator 3.2.2 and IBM MQ Operator 2.0.24	Partial String Comparison	3.2.2 and 2.0.24	N/A	https://www.ibm.com/docs/en/ibm-mq/9.2?topic=openshift-operating-mq-using-mq-operator https://www.ibm.com/support/pages/node/7159714
https://nvd.nist.gov/vuln/detail/CVE-2024-39934	**7.8**	Robotmk (The official Robot Framework integration for	allows a local user to escalate	before 2.0.1	N/A	https://www.robotmk.org/en/ https://checkmk.com/wer

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**
		Checkmk)	privileges			k/16434
https://nvd.nist.gov/vuln/detail/CVE-2024-32853	**7.8**	Dell PowerScale OneFS	execution with unnecessary privileges	versions 8.2.2.x through 9.7.0.2	N/A	https://www.delltechnologies.com/asset/en-gb/products/storage/industry-market/h10719-wp-powerscale-onefs-technical-overview.pdf https://www.dell.com/support/kbdoc/en-us/000226569/dsa-2024-255-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2024-4679	**7.8**	Hitachi JP1/Extensible SNMP Agent for Windows,	Incorrect Default Permissions	N/A	N/A	https://www.tenable.com/cve/CVE-2024-4679 https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-

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**
						2024-127/index.html
https://nvd.nist.gov/vuln/detail/CVE-2024-4944	**7.8**	WatchGuard Mobile VPN	Command Injection	N/A	N/A	https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/mvpn/ssl/mvpn_ssl_client-install_c.html https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00010
https://nvd.nist.gov/vuln/detail/CVE-2024-37999	**7.8**	Medicalis Workflow Orchestrator	Improper Ownership Management	N/A	N/A	https://www.siemens-healthineers.com/digital-health-solutions/medicalis/workflow-orchestrator https://www.siemens-healthineers.com/en-us/support-

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**
						documentation/cybersecurity/shsa-501799
https://nvd.nist.gov/vuln/detail/CVE-2024-39321	**7.5**	Traefik is an HTTP reverse proxy	Authorization Bypass Through User-Controlled Key	Versions prior to 2.11.6, 3.0.4, and 3.1.0-rc3	Versions 2.11.6, 3.0.4, and 3.1.0-rc3	https://traefik.io/traefik/ https://github.com/traefik/traefik/security/advisories/GHSA-gxrv-wf35-62w9
https://nvd.nist.gov/vuln/detail/CVE-2024-6563	**7.5**	Renesas arm-trusted-firmware	Classic Buffer Overflow	N/A	N/A	https://www.renesas.com/us/en/software-tool/hw-rtos?gad_source=1 https://asrg.io/security-advisories/cve-2024-6563/
https://nvd.nist.gov/vuln/detail/CVE-2024-39597	**7.2**	SAP Commerce	Improper Authorization	N/A	N/A	https://www.sap.com/products/crm/commerce-cloud.html https://me.sap.com/notes/3490515 https://url.sap/sapsecurity

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**
						patchday
https://nvd.nist.gov/vuln/detail/CVE-2024-5974	**7.2**	WatchGuard Fireware OS	Classic Buffer Overflow	from 11.9.6 through 12.10.3	N/A	https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/installation/version_upgrade_new_c.html https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00011
https://nvd.nist.gov/vuln/detail/CVE-2024-6409	**7**	OpenSSH server (sshd) Related to CVE-2024-6387	Signal Handler Race Condition	N/A	N/A	https://www.openssh.com/ https://ubuntu.com/security/CVE-2024-6409
https://nvd.nist.gov/vuln/detail/CVE-2024-38330	**7**	IBM System Management for i	Uncontrolled Search Path	7.2, 7.3, and 7.4	N/A	https://www.ibm.com/docs/en/i/7.3?topic=systems-management

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**
			Element			https://www.ibm.com/support/pages/node/7159615

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	**Αναγνωριστικό ευπάθειας**	**URL**
CISA and Partners join ASD'S ACSC to Release Advisory on PRC State-Sponsored Group, APT 40	APT 40 Related	https://www.cisa.gov/news-events/alerts/2024/07/08/cisa-and-partners-join-asds-acsc-release-advisory-prc-state-sponsored-group-apt-40
People's Republic of China (PRC) Ministry of State Security APT40 Tradecraft in Action	APT 40 Related	https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-190a