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-2024-25139	**10**	TP-Link Omada er605	heap-based buffer overflow	1.0.1 through (v2.6) 2.2.3	N/A	https://www.tp-link.com/gr/business-networking/vpn-router/er605/ https://www.tp-link.com/us/omada-sdn/
https://nvd.nist.gov/vuln/detail/CVE-2024-28354	**10**	TRENDnet TEW-827DRU router	command injection	firmware version 2.10B01	N/A	https://www.trendnet.com/products/wireless-router/ac2600-MU-MIMO-WiFi-Router-TEW-827DRU-v2 https://warp-desk-89d.notion.site/TEW-827DRU-c732df50b2454ecaa5451b02f3adda6a
https://nvd.nist.gov/vuln/detail/CVE-2024-34107	**9.8**	Adobe Commerce	Improper Access Control	2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and	N/A	https://business.adobe.com/products/magento/magento-

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**
				earlier		commerce.html https://helpx.adobe.com/security/products/magento/apsb24-40.html
https://nvd.nist.gov/vuln/detail/CVE-2024-26029	**9.8**	Adobe Experience Manager	Improper Access Control	6.5.20 and earlier	N/A	https://business.adobe.com/products/magento/magento-commerce.html https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html
https://nvd.nist.gov/vuln/detail/CVE-2024-7521	**9.8**	Ivanti EPMM	insufficient authorization	prior to 12.1.0.1	N/A	https://help.ivanti.com/mi/help/en_US/core/11.x/gsg/CoreGettingStarted/Core_componen.htm https://forums.ivanti.com/s/article/Security-

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**
						Advisory-Ivanti-Endpoint-Manager-for-Mobile-EPMM-July-2024
https://nvd.nist.gov/vuln/detail/CVE-2024-7521	**9.8**	Firefox , Thunderbird	Incomplete WebAssembly exception handing	Firefox < 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14	N/A	https://www.mozilla.org/en-US/firefox/new/ https://www.mozilla.org/security/advisories/mfsa2024-33/ https://www.mozilla.org/security/advisories/mfsa2024-34/ https://www.mozilla.org/security/advisories/mfsa2024-35/ https://www.mozilla.org/security/advisories/mfsa2024-37/ https://www.mozilla.org/security/advisories/

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**
						mfsa2024-38/
https://nvd.nist.gov/vuln/detail/CVE-2024-7442	**9.8**	Vivotek SD9364 VVTK-0103f	command injection	VVTK-0103f	N/A	https://www.vivotek.com/sd9364-eh-v2 https://vuldb.com/?submit.383843
https://nvd.nist.gov/vuln/detail/CVE-2024-6995	**9.8**	Google Chrome on Android	Inappropriate implementation in Fullscreen	prior to 127.0.6533.72	N/A	https://support.google.com/chrome/answer/95346?hl=en&co=GENIE.Platform%3DAndroid https://issues.chromium.org/issues/343938078
https://nvd.nist.gov/vuln/detail/CVE-	**9.8**	MISP	does not properly check for a valid	before 2.4.187	N/A	https://www.misp-project.org/

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**
2024-29859			file upload			https://github.com/MISP/MISP/commit/238010bfd004680757b324cba0c6344f77a25399
https://nvd.nist.gov/vuln/detail/CVE-2024-38770	**9.8**	Revmakx Backup and Staging by WP Time Capsule	Improper Privilege Management	from n/a through 1.22.20	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-1-22-20-authentication-bypass-and-privilege-escalation-vulnerability?_s_id=cve

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-2024-7350	**9.8**	Appointment Booking Calendar Plugin and Online Scheduling Plugin – BookingPress plugin for WordPress	authentication bypass	1.1.6 to 1.1.7	N/A	https://www.bookingpressplugin.com/ https://www.wordfence.com/threat-intel/vulnerabilities/id/4c367565-75f7-4dd7-a2f1-111df581bd7a?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-23483	**9.8**	Zscaler Client Connector on MacOS	OS Command Injection	MacOS <4.2	N/A	https://www.zscaler.com/platform/zscaler-client-connector https://help.zscaler.com/client-connector/client-connector-app-release-summary-2023?applicable_category=macos&applicable_version=4.2

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-2024-39225	**9.8**	GL-iNet products	remote code execution	AR750/AR750S/AR300M/AR300M16/MT300N-V2/B1300/MT1300/SFT1200/X750 v4.3.11, MT3000/MT2500/AXT1800/AX1800/A1300/X300B v4.5.16, XE300 v4.3.16, E750 v4.3.12, AP1300/S1300 v4.3.13, and XE3000/X3000 v4.4	N/A	https://www.gl-inet.com/products/gl-ar750/ https://github.com/gl-inet/CVE-issues/blob/main/4.0.0/Bypass%20the%20login%20mechanism.md
https://nvd.nist.gov/vuln/detail/CVE-2024-42005	**9.8**	Django 5.0	SQL injection	before 5.0.8 and 4.2 before 4.2.15	N/A	https://docs.djangoproject.com/en/5.0/releases/5.0/ https://docs.djangoproject.com/en/dev/releases/security/

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-2024-28009	**9.8**	NEC Corporation Aterm	execute an arbitrary command with the root privilege via the internet	multiple products	N/A	https://www.qualcomm.com/products/internet-of-things/networking/wi-fi-networks/networking-device-finder/nec-aterm-wx11000t12 https://https//jpn.nec.com/security-info/secinfo/nv24-001_en.html
https://nvd.nist.gov/vuln/detail/CVE-2024-41961	**9.6**	Elektra	Code Injection	N/A	Fixed in commit 8bce00be93b95a6512ff68fe86bf9554e486bc02	https://github.com/sapcc/elektra https://github.com/sapcc/elektra/security/advisories/GHSA-6j2h-486h-487q

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-2024-25331	**9.3**	DIR-822	LAN-Side Unauthenticated Remote Code Execution	Rev. B Firmware v2.02KRB09	N/A	https://support.dlink.com/productinfo.aspx?m=dir-822-us https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10372
https://nvd.nist.gov/vuln/detail/CVE-2024-42348	**9.3**	FOG is a cloning/imaging/rescue suite/inventory management system	leak AD username and password	1.5.10.41.2	1.5.10.41.3 and 1.6.0-beta.1395	https://fogproject.org/ https://github.com/FOGProject/fogproject/security/advisories/GHSA-456c-4gw3-c9xw
https://nvd.nist.gov/vuln/detail/CVE-2024-27181	**8.8**	Apache Linkis	Improper Privilege Management	<= 1.5.0	N/A	https://linkis.apache.org/ https://lists.apache.org/thread/hosd73l7hxb3rpt5rb0yg0ld11zph4c6

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-2024-3238	**8.8**	WordPress Menu Plugin — Superfly Responsive Menu plugin for WordPress	Cross-Site Request Forgery (CSRF)	all versions up to, and including, 5.0.29	N/A	https://codecanyon.net/item/superfly-responsive-wordpress-menu-plugin/8012790 https://www.wordfence.com/threat-intel/vulnerabilities/id/3608fce3-0869-4516-ae08-68108f733c37?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-39634	**8.8**	IdeaBox PowerPack Pro for Elementor	Improper Privilege Management	from n/a through 2.10.14	N/A	https://wordpress.org/plugins/powerpack-lite-for-elementor/ https://patchstack.com/database/vulnerability/powerpack-elements/wordpress-powerpack-pro-for-elementor-plugin-2-

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**
						10-14-contributor-privilege-escalation-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-41616	**8.8**	D-Link DIR-300 REVA	contains hardcoded credentials in the Telnet service	FIRMWARE v1.06B05_WW	N/A	https://www.dlink.com/uk/en/products/dir-300-wireless-g-router https://github.com/LYaoBoL/IOTsec/blob/main/D-Link/DIR300/CVE-2024-41616
https://nvd.nist.gov/vuln/detail/CVE-2024-43199	**8.8**	Nagios NDOUtils	privilege escalation	before 2.1.4	N/A	https://exchange.nagios.org/directory/Addons/Database-Backends/NDOUtils/details https://github.com/NagiosEnterprises/ndoutils/commit/18ef12037f4a

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**
						68772d6840cbaa08aa2da07d2891 https://github.com/NagiosEnterprises/ndoutils/compare/ndoutils-2.1.3...ndoutils-2.1.4 https://github.com/NagiosEnterprises/ndoutils/pull/65
https://nvd.nist.gov/vuln/detail/CVE-2024-6522	**8.5**	Modern Events Calendar plugin for WordPress	Server-Side Request Forgery	all versions up to, and including, 7.12.1	N/A	https://webnus.net/modern-events-calendar/ https://www.wordfence.com/threat-intel/vulnerabilities/id/00bf8f2f-6ab4-4430-800b-5b97abe7589e?source=cve
https://nvd.nist.gov/vuln/detail/CVE-	**8.2**	Omnivise T3000	Cleartext Storage of Sensitive	All versions	N/A	https://www.siemens-energy.com/global/en/

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**
2024-38877		Application Server	Information			home/products-services/product/omnivise-t3000.html https://cert-portal.siemens.com/productcert/html/ssa-857368.html
https://nvd.nist.gov/vuln/detail/CVE-2024-7409	**7.5**	QEMU NBD Server	DoS	N/A	N/A	https://www.qemu.org/docs/master/tools/qemu-nbd.html https://access.redhat.com/security/cve/CVE-2024-7409
https://nvd.nist.gov/vuln/detail/CVE-2024-7389	**7.5**	Forminator plugin for WordPress i	Insufficiently Protected Credentials	all versions up to, and including, 1.29.1	N/A	https://wordpress.org/plugins/forminator/ https://www.wordfence.com/threat-intel/vulnerabilities/id/0d04b822-a48a-485e-b9b5-

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**
						f5a213307c71?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-41827	**7.4**	JetBrains TeamCity	access tokens could continue working after deletion or expiration	before 2024.07	N/A	https://www.jetbrains.com/teamcity https://www.jetbrains.com/privacy-security/issues-fixed/

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	**Αναγνωριστικό ευπάθειας**	**URL**
CISA Releases One Industrial Control Systems Advisory	ICSA-24-219-01 Delta Electronics DIAScreen	https://www.cisa.gov/news-events/alerts/2024/08/06/cisa-releases-one-industrial-control-systems-advisory
CISA Adds One Known Exploited Vulnerability to Catalog	CVE-2018-0824 Microsoft COM for Windows Deserialization of Untrusted Data Vulnerability	https://www.cisa.gov/news-events/alerts/2024/08/05/cisa-adds-one-known-exploited-vulnerability-catalog
CISA Releases Nine Industrial Control Systems Advisories	ICSA-24-214-01 Johnson Controls exacqVision Client and exacqVision Server ICSA-24-214-02 Johnson Controls exacqVision Web Service ICSA-24-214-03 Johnson Controls exacqVision Web Service ICSA-24-214-04 Johnson Controls exacqVision Web Service ICSA-24-214-05 Johnson Controls exacqVision Server ICSA-24-214-06 Johnson Controls exacqVision Web Service ICSA-24-214-07 AVTECH IP Camera ICSA-24-214-08 Vonets WiFi Bridges ICSA-24-214-09 Rockwell Automation Logix Controllers	https://www.cisa.gov/news-events/alerts/2024/08/01/cisa-releases-nine-industrial-control-systems-advisories

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	**Αναγνωριστικό ευπάθειας**	**URL**
CISA Adds Two Known Exploited Vulnerabilities to Catalog	CVE-2024-36971 Android Kernel Remote Code Execution Vulnerability CVE-2024-32113 Apache OFBiz Path Traversal Vulnerability	https://www.cisa.gov/news-events/alerts/2024/08/07/cisa-adds-two-known-exploited-vulnerabilities-catalog