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-2024-4262	7.2	Piotnet Addons For Elementor plugin for WordPress	Stored Cross-Site Scripting	all versions up to, and including, 2.4.28	N/A	https://wordpress.org/plugins/piotnet-addons-for-elementor/ https://www.wordfence.com/threat-intel/vulnerabilities/id/812cc8f1-f89e-47c4-b029-f6a3dbc55d70?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-5031	8.5	Memberpress plugin for WordPress	Blind Server-Side Request Forgery	all versions up to, and including, 1.11.29	N/A	https://wordpress.org/plugins/members/ https://www.wordfence.com/threat-intel/vulnerabilities/id/80064e3b-6996-49eb-a475-0ffe0e894f9e?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-3495	9.8	Country State City Dropdown CF7 plugin for WordPress	SQL Injection	versions up to, and including, 2.7.2	N/A	https://wphive.com/plugins/country-state-city-auto-dropdown/ https://www.wordfence.com/threat-intel/vulnerabilities/id/17dc

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**
						acaf-0e2a-4bef-b944-fb7e43d25777?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-4157	7.5	Contact Form Plugin by Fluent Forms for Quiz, Survey, and Drag & Drop WP Form Builder plugin for WordPress	PHP Object Injection	all versions up to, and including, 5.1.15	N/A	https://wordpress.org/plugins/fluentform/ https://www.wordfence.com/threat-intel/vulnerabilities/id/8def156a-f2f2-4640-a1c9-c21c74e1f308?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-5147	9.8	WPZOOM Addons for Elementor (Templates, Widgets) plugin for WordPress	Local File Inclusion	all versions up to, and including, 1.1.37	N/A	https://wordpress.org/plugins/wpzoom-elementor-addons/ https://www.wordfence.com/threat-intel/vulnerabilities/id/f006bb33-d017-445b-9c02-bd848c199671?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-2088	8.5	NextScripts: Social Networks Auto-Poster plugin for WordPress	Sensitive Information Exposure	all versions up to, and including, 4.4.3	N/A	https://www.nextscripts.com/social-networks-auto-poster-for-wordpress/ https://www.wordfence.com/threat-

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**
						intel/vulnerabilities/id/70724bc7-c1f4-4965-8bba-99b2ed21d34b?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-4443	9.8	Business Directory Plugin – Easy Listing Directories for WordPress	SQL Injection	all versions up to, and including, 6.4.2	N/A	https://wordpress.org/plugins/business-directory-plugin/ https://www.wordfence.com/threat-intel/vulnerabilities/id/982fb304-08d6-4195-97a3-f18e94295492?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-3518	8.8	Media Library Assistant plugin for WordPress	SQL Injection	all versions up to, and including, 3.15	N/A	https://wordpress.org/plugins/media-library-assistant/ https://www.wordfence.com/threat-intel/vulnerabilities/id/a7af1a03-8382-4593-a41f-8cdb1bb9e53b?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-4566	7.1	ShopLentor plugin for WordPress	unauthorized modification of data	all versions up to, and including, 2.8.8	N/A	https://wordpress.org/plugins/woolentor-addons/ https://www.wordfence.com/threat-

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**
						intel/vulnerabilities/id/c6aaabe9-4f55-4c01-b350-573e6a944353?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-4779	8.8	Unlimited Elements For Elementor (Free Widgets, Addons, Templates)	SQL Injection	all versions up to, and including, 1.5.107	N/A	https://wordpress.org/plugins/unlimited-elements-for-elementor/ https://www.wordfence.com/threat-intel/vulnerabilities/id/b155f8ca-9d09-47d7-a7c2-7744df029c19?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-0867	8.1	Email Log plugin for WordPress	Unauthenticated Hook Injection	all versions up to, and including, 2.4.8	N/A	https://wordpress.org/plugins/email-log/ https://www.wordfence.com/threat-intel/vulnerabilities/id/fd15268f-7e06-4e0d-baaf-f27348af61ce?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-4544	9.8	Pie Register - Social Sites Login	authentication bypass	up to, and including, 1.7.7	N/A	https://pieregister.com/ https://www.wordfence.com/threat-intel/vulnerabilities/id/b981

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
						79c3-8b32-4d75-9f3f-2367215a740b?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-4471	8	140+ Widgets | Best Addons For Elementor – FREE for WordPress	PHP Object Injection	up to, and including, 1.4.3.1	N/A	https://wordpress.org/plugins/xpro-elementor-addons/ https://www.wordfence.com/threat-intel/vulnerabilities/id/5c517278-9d2a-4ef6-bf0e-a62f6b00dd20?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-25724	7.3	RTI Connext Professional	buffer overflow	5.3.1 through 6.1.0 before 6.1.1	N/A	https://www.rti.com/products/connext-professional https://community.rti.com/static/documentation/connext-dds/current/doc/vulnerabilities/index.html#cve-2024-25724
https://nvd.nist.gov/vuln/detail/CVE-2024-22274	7.2	vCenter Server	authenticated remote code execution	N/A	N/A	https://www.vmware.com/products/vcenter.html https://support.broadcom.com/web/ecx/support-content-notification/-

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/content/SecurityAdvisories/0/24308
https://nvd.nist.gov/vuln/detail/CVE-2024-22273	8.1	VMware ESXi, Workstation, and Fusion	out-of-bounds read	N/A	N/A	https://www.vmware.com/products/esxi-and-esx.html https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24308
https://nvd.nist.gov/vuln/detail/CVE-2024-31989	9	Argo CD	Use of a Broken or Risky Cryptographic Algorithm	N/A	2.8.19, 2.9.15 and 2.10.10	https://argo-cd.readthedocs.io/en/stable/ https://github.com/argoproj/argo-cd/security/advisories/GHSA-9766-5277-j5hr
https://nvd.nist.gov/vuln/detail/CVE-2024-27130	7.2	QNAP operating system	without checking size of input	N/A	5.1.7.2770 build 20240520 and later QuTS hero h5.1.7.2770	https://www.qnap.com/qts/5.0/en/ https://www.qnap.com/en/security-advisory/qsa-24-23

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**
					build 20240520 and later	
https://nvd.nist.gov/vuln/detail/CVE-2023-3943	10	ZkTeco-based OEM devices	Stack-based Buffer Overflow	ZkTeco-based OEM devices (ZkTeco ProFace X, Smartec ST-FR043, Smartec ST-FR041ME and possibly others)	N/A	https://www.zkteco.com/en/ https://github.com/klsecservices/Advisories/blob/master/K-ZkTeco-2023-006.md
https://nvd.nist.gov/vuln/detail/CVE-2024-30280	7.8	Acrobat Reader	out-of-bounds read	20.005.30574, 24.002.20736 and earlier	N/A	https://get.adobe.com/reader/ https://helpx.adobe.com/security/products/acrobat/apsb24-29.html
https://nvd.nist.gov/vuln/detail/CVE-2024-4835	8	GitLab	Improper Neutralization of Input	versions 15.11 before 16.10.6, 16.11 before 16.11.3, and 17.0 before 17.0.1	N/A	https://about.gitlab.com/ https://gitlab.com/gitlab-org/gitlab/-/issues/461328
https://nvd.nist.gov/vuln/detail/CVE-2024-4347	7.2		Directory Traversal	all versions up to, and including, 1.2.6	N/A	https://wordpress.org/plugins/wp-fastest-cache/

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**
		WP Fastest Cache plugin for WordPress				https://www.wordfence.com/threat-intel/vulnerabilities/id/634d4062-7004-4e89-89a8-323c939aae93?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-29853	7.8	Veeam Agent	authentication bypass	N/A	N/A	https://www.veeam.com/backup-physical-server-trial.html https://veeam.com/kb4582
https://nvd.nist.gov/vuln/detail/CVE-2024-29849	9.8	Veeam Backup Enterprise Manager	log in as any user	N/A	N/A	https://helpcenter.veeam.com/docs/backup/em/introduction.html?ver=120 https://veeam.com/kb4581
https://nvd.nist.gov/vuln/detail/CVE-2024-4454	7.3	WithSecure Elements Endpoint Protection Link	Improper Link Resolution	N/A	N/A	https://www.withsecure.com/en/solutions/software-and-services/elements-endpoint-protection https://www.zerodayinitiative.com/advisories/ZDI-24-491/

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-2024-20360	8.8	Cisco Firepower Management Center	SQL injection	N/A	N/A	https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-sqli-WFFDnNOs
https://nvd.nist.gov/vuln/detail/CVE-2024-27264	7.4	IBM Performance Tools	gain elevated privileges	i 7.2, 7.3, 7.4, and 7.5	N/A	https://www.ibm.com/docs/en/i/7.5?topic=data-performance-tools-i https://www.ibm.com/support/pages/node/7154595
https://nvd.nist.gov/vuln/detail/CVE-2023-51637	9.8	Sante PACS Server PG Patient	SQL Injection	N/A	N/A	https://www.santesoft.com/win/sante-pacs-server-pg/sante-pacs-server-pg.html

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://www.zerodayinitiative.com/advisories/ZDI-24-468/
https://nvd.nist.gov/vuln/detail/CVE-2024-5299	8.8	D-Link D-View	Exposed Dangerous Method or Function	N/A	N/A	https://dview.dlink.com/ https://www.zerodayinitiative.com/advisories/ZDI-24-450/
https://nvd.nist.gov/vuln/detail/CVE-2024-5295	8.8	D-Link G416	OS Command Injection	N/A	N/A	https://www.dlink.com/gr/el/products/g416-eagle-pro-ai-ax1500-4g-cat-6-smart-router https://www.zerodayinitiative.com/advisories/ZDI-24-446/
https://nvd.nist.gov/vuln/detail/CVE-2024-5293	8.8	D-Link DIR-2640	Stack-Based Buffer Overflow	N/A	N/A	https://www.dlink.com/en/products/dir-2640-smart-ac2600-high-power-wi-fi-gigabit-mesh-router https://www.zerodayinitiative.com/advisories/ZDI-24-444/

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-2024-5291	9.8	D-Link DIR-2150	OS Command Injection	N/A	N/A	https://www.dlink.com/ro/ro/products/dir-2150-ac2100-mu-mimo-wi-fi-router https://www.zerodayinitiative.com/advisories/ZDI-24-442/
https://nvd.nist.gov/vuln/detail/CVE-2024-5292	7.3	D-Link Network Assistant	Uncontrolled Search Path Element	N/A	N/A	https://www.dlink.com/uk/en/products/dna https://www.zerodayinitiative.com/advisories/ZDI-24-443/
https://nvd.nist.gov/vuln/detail/CVE-2024-5246	8.8	NETGEAR ProSAFE Network Management System	Remote Code Execution	N/A	N/A	https://www.netgear.com/business/wired/switches/accessories/nms300/ https://kb.netgear.com/000066164/Security-Advisory-for-Multiple-Vulnerabilities-on-the-NMS300-PSV-2024-0003-PSV-2024-0004
https://nvd.nist.gov/vuln/detail/CVE-2024-5242	7.5	TP-Link Omada ER605	Stack-based Buffer Overflow	N/A	N/A	https://www.tp-link.com/gr/business-

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**
						networking/vpn-router/er605/ https://www.zerodayinitiative.com/advisories/ZDI-24-501/
https://nvd.nist.gov/vuln/detail/CVE-2024-26139	8.3	OpenCTI	Improper Access Control	N/A	N/A	https://github.com/OpenCTI-Platform/opencti https://github.com/OpenCTI-Platform/opencti/security/advisories/GHSA-qx4j-f4f2-vjw9

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	**Αναγνωριστικό ευπάθειας**	**URL**
Rockwell Automation Encourages Customers to Assess and Secure Public-Internet-Exposed Assets		https://www.cisa.gov/news-events/alerts/2024/05/21/rockwell-automation-encourages-customers-assess-and-secure-public-internet-exposed-assets
CISA Releases Industrial Control Systems Advisory	ICSA-24-142-01 LCDS LAquis SCADA ICSA-24-144-01 AutomationDirect Productivity PLCs	https://www.cisa.gov/news-events/alerts/2024/05/21/cisa-releases-one-industrial-control-systems-advisory https://www.cisa.gov/news-events/alerts/2024/05/23/cisa-releases-one-industrial-control-systems-advisory
CISA Adds One Known Exploited Vulnerability to Catalog	CVE-2020-17519 Apache Flink Improper Access Control Vulnerability	https://www.cisa.gov/news-events/alerts/2024/05/23/cisa-adds-one-known-exploited-vulnerability-catalog