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-2024-36388	**10**	MileSight DeviceHub	Authentication Bypass	N/A	N/A	https://www.milesight.com/iot/product/devicehub https://www.gov.il/en/Departments/faq/cve_advisories
https://nvd.nist.gov/vuln/detail/CVE-2024-3820	**10**	wpDataTables – WordPress Data Table, Dynamic Tables & Table Charts Plugin plugin for WordPress	SQL Injection	all versions up to, and including, 6.3.1	N/A	https://el.wordpress.org/plugins/wpdatatables/ https://www.wordfence.com/threat-intel/vulnerabilities/id/fbba822b-172f-4167-bccf-4697a298178e?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-25600	**10**	Codeer Limited Bricks Builder	Code Injection	from n/a through 1.9.6	N/A	https://bricksbuilder.io/ https://snicco.io/vulnerability-disclosure/bricks/unauthenticated-rce-in-bricks-1-9-6
https://nvd.nist.gov/vuln/detail/CVE-2024-3200	**9.9**	wpForo Forum plugin for WordPress	SQL Injection	all versions up to, and including, 2.3.3	N/A	https://wordpress.org/plugins/wpforo/ https://www.wordfence.co

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
						m/threat-intel/vulnerabilities/id/f54cdad2-88db-4604-8064-fa6175176760?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-5404	9.8	moneo: IIoT platform	Weak Password Recovery	N/A	N/A	https://www.ifm.com/de/en/shared/moneo-iiot-platform/faqs/faq-moneo-sicherheit-und-support https://cert.vde.com/en/advisories/VDE-2024-028/
https://nvd.nist.gov/vuln/detail/CVE-2024-5311	9.8	DigiWin EasyFlow .NET	SQL Injection	N/A	N/A	https://digiwin.com.my/2021/05/18/enterprise-online-operation-guide%EF%BC%9A-easyflow/ https://www.twcert.org.tw/tw/cp-132-7844-52dad-1.html
https://nvd.nist.gov/vuln/detail/CVE-2024-36108	9.8	casgate is an Open Source Identity and	Improper Authorization	N/A	N/A	https://github.com/casgate/casgate https://github.com/casgat

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
		Access Management				e/casgate/security/advisories/GHSA-mj5q-rc67-h56c
https://nvd.nist.gov/vuln/detail/CVE-2024-23692	9.8	Rejetto HTTP File Server	Improper Neutralization of Special Elements	up to and including version 2.3m	N/A	https://rejetto.com/hfs/ https://mohemiv.com/all/rejetto-http-file-server-2-3m-unauthenticated-rce/
https://nvd.nist.gov/vuln/detail/CVE-2024-4743	9.8	LifterLMS – WordPress LMS Plugin	SQL Injection	all versions up to, and including, 7.6.2	N/A	https://wordpress.org/plugins/lifterlms/ https://www.wordfence.com/threat-intel/vulnerabilities/id/7e3a1e3c-eba0-4ef4-bcb8-929799bb56a8?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-4295	9.8	Email Subscribers by Icegram Express plugin for WordPress	SQL Injection	all versions up to, and including, 5.7.20	N/A	https://wordpress.org/plugins/email-subscribers/ https://www.wordfence.com/threat-intel/vulnerabilities/id/641123af-1ec6-4549-a58c-0a08b4678f45?source=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-2024-35700	9.8	DeluxeThemes Userpro	Improper Privilege Management	from n/a through 5.1.8	N/A	https://codecanyon.net/item/userpro-user-profiles-with-social-login/5958681 https://patchstack.com/database/vulnerability/userpro/wordpress-userpro-plugin-5-1-8-unauthenticated-account-takeover-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-4552	9.8	Social Login Lite For WooCommerce plugin for WordPress	authentication bypass	up to, and including, 1.6.0	N/A	https://woocommerce.com/products/woocommerce-social-login/ https://www.wordfence.com/threat-intel/vulnerabilities/id/f91d6ad6-82fc-4507-90e2-aedfff26bac5?source=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-2024-29974	9.8	Zyxel NAS326	Unrestricted Upload of File	firmware versions before V5.21(AAZF.17)C0 and NAS542 firmware versions before V5.21(ABAG.14)C0	N/A	https://www.zyxelguard.com/NAS326.asp https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-nas-products-06-04-2024
https://nvd.nist.gov/vuln/detail/CVE-2024-29826	9.6	Core server of Ivanti EPM 2022 SU5	SQL Injection	N/A	N/A	https://download.ivanti.com/downloads/Readme/Pages/EPM2022-SU5.html https://forums.ivanti.com/s/article/Security-Advisory-May-2024
https://nvd.nist.gov/vuln/detail/CVE-2024-4008	9.6	FDSK Leak in ABB, Busch-Jaeger, FTS Display	Exposure of Sensitive Information	version 1.00) and BCU (version 1.3.0.33)	N/A	https://global.abb/group/en https://library.e.abb.com/public/7eb3195915744d8d8b4bff5f5bc41cf0/ABBVREP0146_SI_EN_V1-0_9AKK108464A0803_Rev_A.pdf

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-2023-43538 https://nvd.nist.gov/vuln/detail/CVE-2023-43556	**9.3**	TZ Secure OS Memory corruption in Hypervisor	Classic Buffer Overflow	N/A	N/A	https://www.qualcomm.com/ https://docs.qualcomm.com/product/publicresources/securitybulletin/june-2024-bulletin.html
https://nvd.nist.gov/vuln/detail/CVE-2023-33930	**9.1**	Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates)	Unrestricted Upload of File	from n/a through 1.5.66	N/A	https://wordpress.org/plugins/unlimited-elements-for-elementor/ https://patchstack.com/database/vulnerability/unlimited-elements-for-elementor/wordpress-unlimited-elements-for-elementor-plugin-1-5-66-unrestricted-zip-extraction-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-5153	**9.1**	Startklar Elementor Addons plugin for WordPress	Directory Traversal	all versions up to, and including, 1.7.15	N/A	https://wordpress.org/plugins/startklar-elmentor-forms-extwidgets/advanced/

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.wordfence.com/threat-intel/vulnerabilities/id/baa20290-9c01-4f8d-adeb-fbfb15b9d6a9?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-34551	9	Select-Themes Stockholm	Path Traversal	from n/a through 9.6	N/A	https://themeforest.net/item/stockholm-a-genuinely-multiconcept-theme/8819050 https://patchstack.com/database/vulnerability/stockholm/wordpress-stockholm-theme-9-6-unauthenticated-local-file-inclusion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-33560	9	8theme Xstore	Path Traversal	from n/a through 9.3.8	N/A	https://themeforest.net/item/xstore-responsive-woocommerce-theme/15780546 https://patchstack.com/database/vulnerability/xstor

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
						e/wordpress-xstore-theme-9-3-5-unauthenticated-local-file-inclusion-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-5348	8.8	Elements For Elementor plugin for WordPress	Local File Inclusion	all versions up to, and including, 2.2	N/A	https://wordpress.org/plugins/addon-elements-for-elementor-page-builder/ https://www.wordfence.com/threat-intel/vulnerabilities/id/e55b86e2-b42e-483d-93cd-2f09af64dbc7?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-3564	8.8	Content Blocks (Custom Post Widget) plugin for WordPress	Local File Inclusion	all versions up to, and including, 3.3.0	N/A	https://wordpress.org/plugins/custom-post-widget/ https://www.wordfence.com/threat-intel/vulnerabilities/id/c5a0b8fe-d284-4780-84b5-2e97fa96c99a?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-22059	8.8	Ivanti Neurons for ITSM	SQL injection	N/A	N/A	https://www.ivanti.com/products/ivanti-neurons-

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
						itsm https://forums.ivanti.com/s/article/Security-Advisory-May-2024
https://nvd.nist.gov/vuln/detail/CVE-2024-37060	8.8	MLflow platform	Deserialization of Untrusted Data	1.27.0 or newer	N/A	https://mlflow.org/ https://hiddenlayer.com/sai-security-advisory/mlflow-june2024
https://nvd.nist.gov/vuln/detail/CVE-2024-5324	8.8	Login/Signup Popup (Inline Form + Woocommerce) plugin for WordPress	unauthorized modification of data	2.7.1 to 2.7.2	N/A	https://wordpress.org/plugins/easy-login-woocommerce/ https://www.wordfence.com/threat-intel/vulnerabilities/id/005a27c6-b9eb-466c-b0c3-ce52c25bb321?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-35142	8.4	IBM Security Verify Access Docker	Execution with Unnecessary Privileges	10.0.0 through 10.0.6	N/A	https://docs.verify.ibm.com/ibm-security-verify-access/docs/deployment-docker https://www.ibm.com/sup

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
						port/pages/node/7155356
https://nvd.nist.gov/vuln/detail/CVE-2023-38551	8.2	Ivanti Connect Secure	CRLF Injection	9.x, 22.x	N/A	https://www.ivanti.com/products/connect-secure-vpn https://forums.ivanti.com/s/article/Security-Advisory-May-2024
https://nvd.nist.gov/vuln/detail/CVE-2024-36129	8.2	OpenTelemetry Collector	Improper Restriction of Operations	N/A	N/A	https://opentelemetry.io/docs/collector/ https://opentelemetry.io/blog/2024/cve-2024-36129
https://nvd.nist.gov/vuln/detail/CVE-2024-29170	8.1	Dell PowerScale OneFS	Use of Hard-coded Credentials	8.2.x through 9.8.0.x	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/000225667/dsa-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
						210-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2024-23667	7.8	Fortinet FortiWebManager	Improper Authorization	version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and 6.0.2	N/A	https://docs.fortinet.com/document/fortiweb-manager-private-cloud/6.2.3/fortiweb-manager-vm-on-kvm/485484/download-the-fortiweb-manager-vm-software https://fortiguard.fortinet.com/psirt/FG-IR-23-222
https://nvd.nist.gov/vuln/detail/CVE-2024-22058	7.8	Ivanti EPM Agent	buffer overflow	EPM 2021.1 and older	N/A	https://forums.ivanti.com/s/article/Ivanti-Endpoint-Manager-and-Endpoint-Security-Agent-Deployment-Landing-Page?language=en_US https://forums.ivanti.com/s/article/CVE-2024-22058-

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
						Privilege-Escalation-for-Ivanti-Endpoint-Manager-EPM
https://nvd.nist.gov/vuln/detail/CVE-2023-38042	7.8	Ivanti Secure Access Client for Windows	local privilege escalation	N/A	N/A	https://www.ivanti.com/products/connect-secure-vpn https://forums.ivanti.com/s/article/Security-Advisory-May-2024
https://nvd.nist.gov/vuln/detail/CVE-2024-34171	7.8	Fuji Electric Monitouch V-SFT	Stack-based Buffer Overflow	N/A	N/A	https://monitouch.fujielectric.com/site/vsft-e/ https://www.cisa.gov/news-events/ics-advisories/icsa-24-151-02
https://nvd.nist.gov/vuln/detail/CVE-2024-5000 https://nvd.nist.gov/vuln/detail/CVE-2023-5751	7.8	CODESYS products	Incorrect Calculation of Buffer Size	N/A	N/A	https://www.codesys.com/products.html https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=18355&token=e3e5a937ce72602bec39718ddc2f4ba6d983ccd1

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
						&download= https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=18354&token=f3e92a942c3a2f90c272a5ded7598c6a0b5f4924&download=
https://nvd.nist.gov/vuln/detail/CVE-2024-4084	7.7	mintplex-labs/anything-llm	Server-Side Request Forgery (SSRF)	N/A	N/A	https://github.com/Mintplex-Labs/anything-llm https://huntr.com/bounties/bf44517e-a07d-4f54-89b4-3b05fca2a008
https://nvd.nist.gov/vuln/detail/CVE-2024-5526	7.7	Grafana OnCall	Server-Side Request Forgery (SSRF)	from version 1.1.37 before 1.5.2	1.5.2	https://grafana.com/products/cloud/oncall/ https://grafana.com/security/security-advisories/cve-2024-5526/
https://nvd.nist.gov/vuln/detail/CVE-2024-35630	7.6	LJ Apps WP TripAdvisor Review Slider	SQL Injection	from n/a through 12.6	N/A	https://wordpress.org/plugins/wp-tripadvisor-review-slider/ https://patchstack.com/database/vulnerability/wp-

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
						tripadvisor-review-slider/wordpress-wp-tripadvisor-review-slider-plugin-12-6-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-4148	7.5	lunary-ai/lunary application	Uncontrolled Resource Consumption	version 1.2.10	N/A	https://lunary.ai/ https://huntr.com/bounties/eca4ad45-2a38-4f3c-9ec1-8205cd51be31
https://nvd.nist.gov/vuln/detail/CVE-2024-34363	7.5	Envoy (cloud-native, open source edge and service proxy)	Uncaught Exception	N/A	N/A	https://www.envoyproxy.io/ https://github.com/envoyproxy/envoy/security/advisories/GHSA-g979-ph9j-5gg4
https://nvd.nist.gov/vuln/detail/CVE-2024-28996	7.5	SolarWinds Platform	SWQL Injection	N/A	N/A	https://www.solarwinds.com/solarwinds-platform https://www.solarwinds.com/trust-center/security-advisories/CVE-2024-28996

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-2023-46630	7.5	wpase Admin and Site Enhancements (ASE)	Improper Authentication	from n/a through 5.7.1	N/A	https://www.wpase.com/ https://patchstack.com/database/vulnerability/admin-site-enhancements/wordpress-admin-and-site-enhancements-ase-plugin-5-7-1-password-protected-view-bypass-vulnerability-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-4540	7.5	Keycloak	Exposure of Sensitive Information	N/A	N/A	https://www.keycloak.org/ https://bugzilla.redhat.com/show_bug.cgi?id=2279303
https://nvd.nist.gov/vuln/detail/CVE-2024-36128	7.5	Directus	Improper Check for Unusual or Exceptional Conditions	Prior to 10.11.2	N/A	https://directus.io/ https://github.com/directus/directus/security/advisories/GHSA-632p-p495-25m5
https://nvd.nist.gov/vuln/detail/CVE-2024-5037	7.5	OpenShift's Telemeter	Authentication Bypass by	N/A	N/A	https://github.com/openshift/telemeter

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
			Spoofing			https://access.redhat.com/security/cve/CVE-2024-5037
https://nvd.nist.gov/vuln/detail/CVE-2024-3667	7.4	Brizy – Page Builder plugin for WordPress	Stored Cross-Site Scripting	all versions up to, and including, 2.4.43	N/A	https://wordpress.org/plugins/brizy/ https://www.wordfence.com/threat-intel/vulnerabilities/id/f0edfebc-bf6b-4346-9cd7-ce00007e3620?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-29848	7.2	Ivanti Avalanche	unrestricted file upload	before 6.4.x	N/A	https://www.avax.network/ https://forums.ivanti.com/s/article/Security-Advisory-May-2024
https://nvd.nist.gov/vuln/detail/CVE-2024-20404	7.2	Cisco Finesse	Server-Side Request Forgery (SSRF)	N/A	N/A	https://www.cisco.com/c/en/us/products/contact-center/finesse/index.html https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor

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
						y/cisco-sa-finesse-ssrf-rfi-Um7wT8Ew
https://nvd.nist.gov/vuln/detail/CVE-2024-1662	7.2	PORTY Smart Tech Technology Joint Stock Company PowerBank Application	Exposure of Sensitive Information	before 2.02	N/A	https://porty.tech/en/main-page https://www.usom.gov.tr/bildirim/tr-24-0602
https://nvd.nist.gov/vuln/detail/CVE-2024-35631	7.1	Foliovision FV Flowplayer Video Player	Cross-site Scripting	from n/a through 7.5.45.7212	N/A	https://en-gb.wordpress.org/plugins/fv-wordpress-flowplayer/ https://patchstack.com/database/vulnerability/fv-wordpress-flowplayer/wordpress-fv-flowplayer-video-player-plugin-7-5-45-7212-cross-site-scripting-xss-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-2024-4958	7.1	User Registration – Custom Registration Form, Login Form, and User Profile WordPress Plugin plugin	unauthorized modification of data	versions up to, and including, 3.2.0.1	N/A	https://wordpress.org/plugins/user-registration/ https://www.wordfence.com/threat-intel/vulnerabilities/id/710574a8-a6e2-4ee6-9ea7-03a34994fec7?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-35668	7.1	Brevo Newsletter, SMTP, Email marketing and Subscribe forms by Sendinblue	Cross-site Scripting	from n/a through 3.1.77	N/A	https://wordpress.org/plugins/mailin/ https://patchstack.com/database/vulnerability/mailin/wordpress-newsletter-smtp-email-marketing-and-subscribe-forms-by-brevo-plugin-3-1-77-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-35664	7.1	WPvivid Team WPvivid Backup for MainWP	Cross-site Scripting	from n/a through 0.9.32	N/A	https://wordpress.org/plugins/wpvivid-backup-mainwp/ https://patchstack.com/d

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
						atabase/vulnerability/wpvivid-backup-mainw/wordpress-wpvivid-backup-for-mainwp-plugin-0-9-32-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας	URL
CISA Releases Four Industrial Control Systems Advisories	ICSA-24-156-01 Uniview NVR301-04S2-P4 ICSA-23-278-03 Mitsubishi Electric CC-Link IE TSN Industrial Managed Switch (Update A) ICSA-22-172-01 Mitsubishi Electric MELSEC iQ-R, Q, L Series and MELIPC Series (Update C) ICSA-24-151-02 Fuji Electric Monitouch V-SFT (Update A)	https://www.cisa.gov/news-events/alerts/2024/06/04/cisa-releases-four-industrial-control-systems-advisories
CISA Adds One Known Exploited	CVE-2017-3506 Oracle WebLogic Server OS Command	https://www.cisa.gov/news-

Vulnerability to Catalog	Injection Vulnerability	events/alerts/2024/06/03/cisa-adds-one-known-exploited-vulnerability-catalog