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-2024-30299	**10**	Adobe Framemaker Publishing Server	Improper Authentication	2020.3, 2022.2 and earlier	N/A	https://www.adobe.com/gr_en/products/framemaker/publishing-server.html https://helpx.adobe.com/security/products/framemaker-publishing-server/apsb24-38.html
https://nvd.nist.gov/vuln/detail/CVE-2024-3922	**10**	Dokan Pro plugin for WordPress	SQL Injection	all versions up to, and including, 3.10.3	N/A	https://wordpress.org/plugins/dokan-lite/ https://www.wordfence.com/threat-intel/vulnerabilities/id/d9de41de-f2f7-4b16-8ec9-d30bbd3d8786?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-5577	**9.8**	Where I Was, Where I Will Be plugin for WordPress	Remote File Inclusion	version <= 1.1.1	N/A	https://wordpress.org/plugins/where-i-was-where-i-will-be/ https://www.wordfence.com/threat-intel/vulnerabilities/id/68e0f54d-08ec-4e41-ac9b-d72cdde5a724?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-2024-4936	**9.8**	Canto plugin for WordPress	Remote File Inclusion	all versions up to, and including, 3.0.8	N/A	https://wordpress.org/plugins/canto/ https://www.wordfence.com/threat-intel/vulnerabilities/id/95a68ae0-36da-499b-a09d-4c91db8aa338?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-27174	**9.8**	Toshiba Multifunctional Systems and Printers	Remote Code Execution	N/A	N/A	https://www.toshibatec.eu/products/multifunctional-systems-and-printers/ https://www.toshibatec.com/information/pdf/information20240531_01.pdf
https://nvd.nist.gov/vuln/detail/CVE-2024-3080	**9.8**	ASUS router models	Improper Authentication	N/A	N/A	https://www.asus.com/networking-iot-servers/wifi-routers/all-series/ https://www.twcert.org.tw/en/cp-139-7860-760b1-2.html https://www.twcert.org.tw/tw/cp-132-7859-0e104-1.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://nvd.nist.gov/vuln/detail/CVE-2024-34102	**9.8**	Adobe Commerce	Improper Restriction of XML External Entity Reference	2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier	N/A	https://business.adobe.com/products/magento/magento-commerce.html https://helpx.adobe.com/security/products/magento/apsb24-40.html
https://nvd.nist.gov/vuln/detail/CVE-2024-37036	**9.8**	Schneider Electric	Out-of-bounds Write	N/A	N/A	https://www.se.com/ww/en/ https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-163-05&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-163-05.pdf
https://nvd.nist.gov/vuln/detail/CVE-2024-5211	**9.1**	mintplex-labs/anything-llm	Path Traversal	N/A	N/A	https://github.com/Mintplex-Labs/anything-llm https://huntr.com/bounties/38f282cb-7226-435e-9832-2d4a102dad4b

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-2024-0095	**9**	NVIDIA Triton Inference Server	Improper Output Neutralization for Logs	N/A	N/A	https://developer.nvidia.com/triton-inference-server https://nvidia.custhelp.com/app/answers/detail/a_id/5546
https://nvd.nist.gov/vuln/detail/CVE-2024-4371	**9**	CoDesigner WooCommerce Builder for Elementor – Customize Checkout, Shop, Email, Products & More plugin for WordPress	PHP Object Injection	all versions up to, and including, 4.4.1	N/A	https://wordpress.org/plugins/woolementor/ https://www.wordfence.com/threat-intel/vulnerabilities/id/d1e5131a-9e72-441d-971c-8b9af35cf3f7?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-5995	**8.8**	Soar Cloud HR Portal	Insufficient Session Expiration	N/A	N/A	https://www.taiwantrade.com/home.html https://www.twcert.org.tw/en/cp-139-7872-1c8b4-2.html https://www.twcert.org.tw/tw/cp-132-7871-fecf1-1.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://nvd.nist.gov/vuln/detail/CVE-2024-5948	**8.8**	Deep Sea Electronics DSE855	Stack-based Buffer Overflow	DSE855	N/A	https://www.deepseaelectronics.com/genset/remote-communications-overview-displays/dse855 https://www.zerodayinitiative.com/advisories/ZDI-24-672/
https://nvd.nist.gov/vuln/detail/CVE-2024-36396	**8.8**	Verint (Open Platform for CX Automation)	Unrestricted Upload of File with Dangerous Type	N/A	N/A	https://www.verint.com/ https://www.gov.il/en/Departments/faq/cve_advisories
https://nvd.nist.gov/vuln/detail/CVE-2024-25949	**8.8**	Dell OS10 Networking Switches	Improper Authorization	versions10.5.6.x, 10.5.5.x, 10.5.4.x and 10.5.3.x	N/A	https://www.dell.com/en-us/shop/ipovw/open-platform-software https://www.dell.com/support/kbdoc/en-us/000225922/dsa-2024-087-security-update-for-dell-networking-os10-vulnerability

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-2024-4845	**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-2024-4404	**8.5**	ElementsKit PRO plugin for WordPress	Server-Side Request Forgery	versions up to, and including, 3.6.2	N/A	https://wordpress.org/plugins/elementskit-lite/ https://www.wordfence.com/threat-intel/vulnerabilities/id/6417269d-3d49-4f33-b92a-5aacb052bab0?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-32504	**8.4**	Samsung Mobile Processor	lacks proper length checking	Exynos 850, Exynos 1080, Exynos 2100, Exynos 1280, Exynos 1380, Exynos 1330, Exynos W920, Exynos W930	N/A	https://semiconductor.samsung.com/processor/mobile-processor/ https://semiconductor.samsung.com/support/quality-support/product-security-updates/

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-2024-37300	**8.1**	JupyterHub 5.0	Incorrect Authorization	< 5.0	N/A	https://jupyterhub.readthedocs.io/en/latest/howto/upgrading-v5.html https://github.com/jupyterhub/oauthenticator/security/advisories/GHSA-gprj-3p75-f996
https://nvd.nist.gov/vuln/detail/CVE-2024-3183	**8.1**	FreeIPA	Use of Password Hash With Insufficient Computational Effort	N/A	N/A	https://www.freeipa.org/ https://www.freeipa.org/release-notes/4-12-1.html
https://nvd.nist.gov/vuln/detail/CVE-2024-36502	**7.9**	HUAWEI products	Out-of-bounds Read	N/A	N/A	https://consumer.huawei.com/en/tablets/ https://consumer.huawei.com/en/support/bulletin/2024/6/
https://nvd.nist.gov/vuln/detail/CVE-2024-37307	**7.9**	Cilium (a networking, observability, and security solution	Exposure of Sensitive Information	Starting in version 1.13.0 and prior to versions 1.13.7, 1.14.12, and 1.15.6	N/A	https://cilium.io/ https://github.com/cilium/cilium/security/advisories/GHSA-wh78-7948-358j

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**
		with an eBPF-based dataplane)				
https://nvd.nist.gov/vuln/detail/CVE-2024-0099	**7.8**	NVIDIA vGPU	Classic Buffer Overflow	N/A	N/A	https://www.nvidia.com/en-eu/data-center/virtual-solutions/ https://nvidia.custhelp.com/app/answers/detail/a_id/5551
https://nvd.nist.gov/vuln/detail/CVE-2024-37022	**7.8**	Fuji Electric Tellus Lite V-Simulator	Out-of-bounds Write	N/A	N/A	https://monitouch.fujielectric.com/site/tellus-e/ https://www.cisa.gov/news-events/ics-advisories/icsa-24-165-14
https://nvd.nist.gov/vuln/detail/CVE-2024-34115	**7.8**	Adobe Substance3D - Stager	Out-of-bounds Write	versions 2.1.4 and earlier	N/A	https://www.adobe.com/gr_en/products/substance3d-stager.html https://helpx.adobe.com/security/products/substance3d_stager/apsb24-43.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://nvd.nist.gov/vuln/detail/CVE-2024-20753	**7.8**	Adobe Photoshop Desktop	Out-of-bounds Read	24.7.3, 25.7 and earlier	N/A	https://www.adobe.com/gr_en/products/photoshop/landpa.html https://helpx.adobe.com/security/products/photoshop/apsb24-27.html
https://nvd.nist.gov/vuln/detail/CVE-2024-28964	**7.8**	Dell Common Event Enabler	Deserialization of Untrusted Data	version 8.9.10.0 and prior	N/A	https://www.dell.com/support/home/en-us/product-support/product/common-event-enabler/docs https://www.dell.com/support/kbdoc/en-us/000224987/dsa-2024-179-security-update-for-dell-emc-common-event-enabler-windows-for-cavatools-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2024-5551	**7.5**	WP STAGING Pro WordPress Backup Plugin plugin for WordPress	Cross-Site Request Forgery	all versions up to, and including, 5.6.0	N/A	https://wp-staging.com/ https://www.wordfence.com/threat-intel/vulnerabilities/id/2a99a21c-d4f1-4cdb-b1f1-

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**
						31b3cf666b80?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-4696	**7.5**	Lenovo Service Bridge	OS Command Injection	prior to version 5.0.2.17	N/A	https://support.lenovo.com/us/en/solutions/ht104055-lenovo-service-bridge-automatically-detects-your-system-type-and-serial-number-for-an-improved-lenovo-support-experience https://support.lenovo.com/us/en/product_security/LEN-163429
https://nvd.nist.gov/vuln/detail/CVE-2024-37131	**7.5**	Dell SCG Policy Manager	Permissive Cross-domain Policy with Untrusted Domains	N/A	N/A	https://www.dell.com/support/manuals/en-us/secure-connect-gateway-ve/pm_5.x_ug/download-policy-manager-for-secure-connect-gateway https://www.dell.com/support/kbdoc/en-us/000225956/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**
						254-security-update-for-dell-secure-connect-gateway-policy-manager-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2024-32859	**7.5**	Dell Client Platform BIOS	Improper Input Validation	N/A	N/A	https://www.dell.com/support/kbdoc/en-uk/000221745/dsa-2024-067 https://www.dell.com/support/kbdoc/en-us/000223439/dsa-2024-124
https://nvd.nist.gov/vuln/detail/CVE-2024-34112	**7.5**	Adobe ColdFusion	Improper Access Control	2023u7, 2021u13 and earlier	N/A	https://www.adobe.com/gr_en/products/coldfusion-family.html https://helpx.adobe.com/security/products/coldfusion/apsb24-41.html
https://nvd.nist.gov/vuln/detail/CVE-2024-30472	**7.5**	Dell ThinOS	Exposure of Sensitive Information	v1.0.0.8	N/A	https://www.dell.com/en-us/lp/dell-thinos https://www.dell.com/support/kbdoc/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**
						us/000225289/dsa-2024-229
https://nvd.nist.gov/vuln/detail/CVE-2024-26029	**7.5**	Adobe Experience Manager	Improper Access Control	versions 6.5.20 and earlier	N/A	https://business.adobe.com/au/products/experience-manager/adobe-experience-manager.html https://helpx.adobe.com/security/products/experience-manager/apsb24-28.html
https://nvd.nist.gov/vuln/detail/CVE-2024-2098	**7.5**	Download Manager plugin for WordPress	unauthorized access of data	all versions up to, and including, 3.2.89	N/A	https://wordpress.org/plugins/download-manager/ https://www.wordfence.com/threat-intel/vulnerabilities/id/1301c8af-d81a-40f1-96fa-e8252309d8a4?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-31162	**7.2**	ASUS Download Master	OS Command Injection	N/A	N/A	https://www.asus.com/support/faq/114001/ https://www.twcert.org.tw/en/cp-139-7868-8a760-2.html https://www.twcert.org.tw/t

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
						w/cp-132-7867-8fad9-1.html

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	**Αναγνωριστικό ευπάθειας**	**URL**
CISA Releases Twenty Industrial Control Systems Advisories	ICSA-24-165-01 Siemens Mendix Applications ICSA-24-165-02 Siemens SIMATIC S7-200 SMART Devices ICSA-24-165-03 Siemens TIA Administrator ICSA-24-165-04 Siemens ST7 ScadaConnect ICSA-24-165-05 Siemens SITOP UPS1600 ICSA-24-165-06 Siemens TIM 1531 IRC ICSA-24-165-07 Siemens PowerSys ICSA-24-165-08 Siemens Teamcenter Visualization and JT2Go ICSA-24-165-09 Siemens SICAM AK3/BC/TM ICSA-24-165-10 Siemens SIMATIC and SIPLUS ICSA-24-165-11 Siemens SCALANCE XM-400, XR-500 ICSA-24-165-12 Siemens SCALANCE W700 ICSA-24-165-13 Siemens SINEC Traffic Analyzer ICSA-24-165-14 Fuji Electric Tellus Lite V-Simulator ICSA-24-165-16 Rockwell Automation FactoryTalk View SE ICSA-24-165-17 Rockwell Automation FactoryTalk View SE ICSA-24-165-18 Rockwell Automation FactoryTalk View SE ICSA-24-165-19 Motorola Solutions Vigilant License Plate Readers ICSA-24-074-14 Mitsubishi Electric MELSEC-Q/L Series (Update B) ICSA-20-245-01 Mitsubishi Electric Multiple Products (Update G)	https://www.cisa.gov/news-events/alerts/2024/06/13/cisa-releases-twenty-industrial-control-systems-advisories

CISA Adds Known Exploited Vulnerabilities to Catalog	CVE-2024-32896 Android Pixel Privilege Escalation Vulnerability CVE-2024-26169 Microsoft Windows Error Reporting Service Improper Privilege Management Vulnerability CVE-2024-4358 Progress Telerik Report Server Authentication Bypass by Spoofing Vulnerability CVE-2024-4610 ARM Mali GPU Kernel Driver Use-After-Free Vulnerability CVE-2024-4577 PHP-CGI OS Command Injection Vulnerability	https://www.cisa.gov/news-events/alerts/2024/06/13/cisa-adds-three-known-exploited-vulnerabilities-catalog https://www.cisa.gov/news-events/alerts/2024/06/12/cisa-adds-two-known-exploited-vulnerabilities-catalog