| **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-2024-36412 | **10** | SuiteCRM | SQL Injection | Prior to versions 7.14.4 and 8.6.1 | Versions 7.14.4 and 8.6.1 contain a fix | https://suitecrm.com/<br>https://github.com/salesagility/SuiteCRM/security/advisories/GHSA-xjx2-38hv-5hh8 |
| https://nvd.nist.gov/vuln/detail/CVE-2024-35746 | **10** | Asghar Hatampoor BuddyPress Cover | Code Injection | from n/a through 2.1.4.2 | N/A | https://wphive.com/plugins/bp-cover/<br>https://patchstack.com/database/vulnerability/bp-cover/wordpress-buddypress-cover-plugin-2-1-4-2-arbitrary-file-upload-vulnerability?_s_id=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2024-5480 | **10** | PyTorch | Command Injection | versions prior to 2.2.2 | N/A | https://pytorch.org/<br>https://huntr.com/bounties/39811836-c5b3-4999-831e-46fee8fcade3 |
| https://nvd.nist.gov/vuln/detail/CVE-2024-2013 | **10** | FOXMAN-UN/UNEM server | Authentication Bypass | N/A | N/A | https://www.hitachienergy.com/products-and-solutions/communication-networks/wired-networks/fox-multiservice-platform/foxman<br>https://publisher.hitachienergy.com/preview?DocumentId=8DBD000201&languageCode=en&Preview=true |

| 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-2024-3549 | **9.9** | Blog2Social: Social Media Auto Post & Scheduler plugin for WordPress | SQL Injection | all versions up to, and including, 7.4.1 | N/A | https://wordpress.org/plugins/blog2social/<br>https://www.wordfence.com/threat-intel/vulnerabilities/id/3b472eb8-9808-4a50-b2b4-0b0b3256053f?source=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2024-34762 | **9.9** | WPENGINE INC Advanced Custom Fields PRO | Path Traversal | from n/a before 6.2.10 | N/A | https://www.advancedcustomfields.com/<br>https://patchstack.com/database/vulnerability/advanced-custom-fields-pro/wordpress-advanced-custom-fields-pro-plugin-6-2-10-contributor-local-file-inclusion-vulnerability?_s_id=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2024-3592 | **9.9** | Quiz And Survey Master – Best Quiz, Exam and Survey Plugin for WordPress | SQL Injection | all versions up to, and including, 9.0.1 | N/A | https://wordpress.org/plugins/quiz-master-next/<br>https://www.wordfence.com/threat-intel/vulnerabilities/id/fc085413-db43-43e3-9b60-aeb341eed4e1?source=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2024-37301 | **9.9** | Document Merge Service | Improper Neutralization of Special Elements | N/A | N/A | https://github.com/adfinis/document-merge-service<br>https://github.com/adfinis/document-merge- |

| 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** |
| | | | Used in a Template Engine | | | service/security/advisories/GHSA-v5gf-r78h-55q6 |
| https://nvd.nist.gov/vuln/detail/CVE-2024-4146 | **9.8** | lunary-ai/lunary | Improper Authorization | 1.2.13 | N/A | https://lunary.ai/<br>https://huntr.com/bounties/a749e696-b398-4260-b2d0-b0054b9fffa7 |
| https://nvd.nist.gov/vuln/detail/CVE-2024-4577 | **9.8** | PHP | OS Command Injection | 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8 | N/A | https://www.php.net/<br>https://www.php.net/ChangeLog-8.php#8.1.29 Release Notes<br>https://www.php.net/ChangeLog-8.php#8.2.20 Release Notes<br>https://www.php.net/ChangeLog-8.php#8.3.8 |
| https://nvd.nist.gov/vuln/detail/CVE-2024-3408 | **9.8** | man-group/dtale | Improper Input Validation | 3.10.0 | N/A | https://github.com/man-group/dtale<br>https://huntr.com/bounties/57a06666-ff85-4577-af19-f3dfb7b02f91 |
| https://nvd.nist.gov/vuln/detail/CVE-2024-3149 | **9.6** | mintplex-labs/anything-llm | Server-Side Request Forgery (SSRF) | N/A | N/A | https://github.com/Mintplex-Labs/anything-llm<br>https://github.com/mintplex-labs/anything-llm/commit/f4088d9348fa86dcebe9f97a18d39c0a6e92f15e |

| **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-2024-35225 | **9.6** | Jupyter Server Proxy | Improper Encoding or Escaping of Output | Versions of 3.x prior to 3.2.4 and 4.x prior to 4.2.0 | N/A | https://github.com/jupyterhub/jupyter-server-proxy<br>https://github.com/jupyterhub/jupyter-server-proxy/security/advisories/GHSA-fvcq-4x64-hqxr |
| https://nvd.nist.gov/vuln/detail/CVE-2024-37051 | **9.3** | JetBrains IDEs | Insufficiently Protected Credentials | N/A | N/A | https://www.jetbrains.com/ides/<br>https://www.jetbrains.com/privacy-security/issues-fixed/ |
| https://nvd.nist.gov/vuln/detail/CVE-2024-36266 | **9.3** | PowerSys | Improper Authentication | All versions < V3.11 | N/A | https://global.powersys-solutions.com/<br>https://cert-portal.siemens.com/productcert/html/ssa-024584.html |
| https://nvd.nist.gov/vuln/detail/CVE-2024-33565 | **9.1** | UkrSolution Barcode Scanner | Missing Authorization | from n/a through 1.5.3 | N/A | https://www.ukrsolution.com/Wordpress/WooCommerce-Barcode-QRCode-Scanner-Reader<br>https://patchstack.com/database/vulnerability/barcode-scanner-lite-pos-to-manage-products-inventory-and-orders/wordpress-barcode-scanner-with-inventory-order-manager-plugin-1-5-3-unauthenticated-broken-access- |

| CVEs | | | | | | |
|---|---|---|---|---|---|---|
| URL ευπάθειας (NIST NVD) | CVSSv3 | Προϊόν/Υπηρεσία | Τύπος Ευπάθειας | Συσκευές/Εκδόσεις που επηρεάζονται | Συσκευές/ Εκδόσεις που ΔΕΝ επηρεάζονται | URL προϊόντος/υπηρεσίας<br>URL οδηγιών αντιμετώπισης |
| | | | | | | control-vulnerability?_s_id=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2024-29855 | **9** | Veeam Recovery Orchestrator | authentication bypass | N/A | N/A | https://www.veeam.com/disaster-recovery-orchestrator.html<br>https://www.veeam.com/kb4585 |
| https://nvd.nist.gov/vuln/detail/CVE-2024-35677 | **9** | StylemixThemes MegaMenu | Path Traversal | from n/a through 2.3.12 | N/A | https://stylemixthemes.com/consulting/megamenu/<br>https://patchstack.com/database/vulnerability/stm-megamenu/wordpress-megamenu-plugin-2-3-12-unauthenticated-local-file-inclusion-vulnerability?_s_id=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2024-35213 | **9** | SGI Image Codec of QNX SDP | Improper Input Validation | version(s) 6.6, 7.0, and 7.1 | N/A | https://blackberry.qnx.com/en/products/foundation-software/qnx-software-development-platform<br>https://support.blackberry.com/pkb/s/article/139914 |
| https://nvd.nist.gov/vuln/detail/CVE-2024-33564 | **8.8** | 8theme Xstore | Missing Authorization | from n/a through 9.3.8 | N/A | https://themeforest.net/item/xstore-responsive-woocommerce-theme/15780546<br>https://patchstack.com/database/vulnerability/xstore/wordpress- |

| 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** |
| | | | | | | xstore-theme-9-3-5-arbitrary-option-update-vulnerability?_s_id=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2024-3668 | **8.8** | PowerPack Pro for Elementor plugin for WordPress | privilege escalation | all versions up to, and including, 2.10.17 | N/A | https://wordpress.org/plugins/powerpack-lite-for-elementor/<br>https://www.wordfence.com/threat-intel/vulnerabilities/id/249ccc77-0daf-41bc-b5c5-991bf17d645d?source=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2024-28877 | **8.8** | MicroDicom DICOM Viewer | Stack-based Buffer Overflow | N/A | N/A | https://www.microdicom.com/<br>https://www.cisa.gov/news-events/ics-medical-advisories/icsma-24-163-01 |
| https://nvd.nist.gov/vuln/detail/CVE-2023-52233 | **8.6** | Post SMTP Post SMTP Mailer/Email Log | Missing Authorization | from n/a through 2.8.6 | N/A | https://wordpress.org/plugins/post-smtp/<br>https://patchstack.com/database/vulnerability/post-smtp/wordpress-post-smtp-mailer-plugin-2-8-6-broken-access-control-on-api-vulnerability?_s_id=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2024-32778 | **8.5** | Contest Gallery | Missing Authorization | from n/a through 21.3.4 | N/A | https://www.contest-gallery.com/<br>https://patchstack.com/database/vulnerability/contest-gallery/wordpress-contest-gallery- |

| 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** |
| | | | | | | plugin-21-3-4-arbitrary-file-deletion-vulnerability?_s_id=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2024-31959 | **8.4** | Samsung Mobile Processor Exynos | code execution | Exynos 2200, Exynos 1480, Exynos 2400 | N/A | https://semiconductor.samsung.com/processor/mobile-processor/<br>https://semiconductor.samsung.com/support/quality-support/product-security-updates/ |
| https://nvd.nist.gov/vuln/detail/CVE-2024-33547 | **8.3** | AA-Team Wzone | Missing Authorization | from n/a through 14.0.10 | N/A | https://www.aa-team.com/aa-teamportfolio/<br>https://patchstack.com/database/vulnerability/woozone/wordpress-wzone-plugin-14-0-10-site-wide-broken-access-control-vulnerability?_s_id=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2023-31080 | **8.3** | Unlimited Elements Unlimited Elements For Elementor | Missing Authorization | from n/a through 1.5.65 | N/A | https://wordpress.org/plugins/unlimited-elements-for-elementor/<br>https://patchstack.com/database/vulnerability/unlimited-elements-for-elementor/wordpress-unlimited-elements-for-elementor-plugin-1-5-65-multiple-broken-access-control-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-2024-35292 | **8.2** | SIMATIC S7-200 SMART CPU | Use of Insufficiently Random Values | N/A | N/A | https://cspower.com.my/sabah/wp-content/uploads/2017/02/S7-200-SMART-PLC-catalog.pdf<br>https://cert-portal.siemens.com/productcert/html/ssa-481506.html |
| https://nvd.nist.gov/vuln/detail/CVE-2024-37177 | **8.1** | SAP Financial Consolidation | Cross-site Scripting | N/A | N/A | https://support.sap.com/infopages/swdc/fm/fincons101.html<br>https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html |
| https://nvd.nist.gov/vuln/detail/CVE-2024-4190 | **8.1** | OpenText ArcSight Logger | Cross-site Scripting | N/A | N/A | https://www.microfocus.com/media/data-sheet/arcsight-logger-ds.pdf<br>https://portal.microfocus.com/s/article/KM000030655 |
| https://nvd.nist.gov/vuln/detail/CVE-2024-5785 | **8** | Comtrend router | OS Command Injection | WLD71-T1_v2.0.201820, affecting the GRG-4280us version | N/A | https://us.comtrend.com/category/product/wireless/wireless-routers/<br>https://www.incibe.es/en/incibe-cert/notices/aviso/multiple-vulnerabilities-comtrend-router |
| https://nvd.nist.gov/vuln/detail/CVE-2024-37289 | **7.8** | Trend Micro Apex One | Privilege Escalation | N/A | N/A | https://www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html<br>https://success.trendmicro.com/dc |

| 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** |
| | | | | | | x/s/solution/000298063 |
| https://nvd.nist.gov/vuln/detail/CVE-2024-36358 | **7.8** | Trend Micro Deep Security 20.x | Privilege Escalation | below build 20.0.1-3180 | N/A | https://help.deepsecurity.trendmicro.com/software.html<br>https://success.trendmicro.com/dcx/s/solution/000298151 |
| https://nvd.nist.gov/vuln/detail/CVE-2024-32849 | **7.8** | Trend Micro Security 17.x (Consumer) | Privilege Escalation | 17.x | N/A | https://www.trendmicro.com/en_us/forHome/products/downloads.html<br>https://helpcenter.trendmicro.com/en-us/article/tmka-19175 |
| https://nvd.nist.gov/vuln/detail/CVE-2024-5597 | **7.8** | Fuji Electric Monitouch V-SFT | Type Confusion | N/A | N/A | https://monitouch.fujielectric.com/site/vsft-eu/<br>https://www.cisa.gov/news-events/ics-advisories/icsa-24-151-02 |
| https://nvd.nist.gov/vuln/detail/CVE-2024-23110 | **7.8** | Fortinet FortiOS | Stack-based Buffer Overflow | 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, 6.0 all versions | N/A | https://www.fortinet.com/products/fortigate/fortios<br>https://fortiguard.com/psirt/FG-IR-23-460 |

| CVEs | | | | | | |
|---|---|---|---|---|---|---|
| URL ευπάθειας (NIST NVD) | CVSSv3 | Προϊόν/Υπηρεσία | Τύπος Ευπάθειας | Συσκευές/Εκδόσεις που επηρεάζονται | Συσκευές/ Εκδόσεις που ΔΕΝ επηρεάζονται | URL προϊόντος/υπηρεσίας<br>URL οδηγιών αντιμετώπισης |
| https://nvd.nist.gov/vuln/detail/CVE-2024-32703 | **7.7** | reputeinfosystems ARForms | Missing Authorization | from n/a through 6.4 | N/A | https://www.arformsplugin.com/<br>https://patchstack.com/database/vulnerability/arforms/wordpress-arforms-plugin-6-4-subscriber-arbitrary-file-deletion-vulnerability?_s_id=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2023-32475 | **7.6** | Dell BIOS | Missing Support for Integrity Check | N/A | N/A | https://www.dell.com/support/kbdoc/en-us/000124211/dell-bios-updates<br>https://www.dell.com/support/kbdoc/en-us/000215644/dsa-2023-222-security-update-for-an-amd-bios-vulnerability |
| https://nvd.nist.gov/vuln/detail/CVE-2024-34688 | **7.5** | SAP NetWeaver | Uncontrolled Resource Consumption | N/A | N/A | https://www.sap.com/greece/products/technology-platform/netweaver.html<br>https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html |
| https://nvd.nist.gov/vuln/detail/CVE-2024-32798 | **7.5** | WP Travel Engine | Missing Authorization | from n/a through 5.8.0 | N/A | https://wptravelengine.com/<br>https://patchstack.com/database/vulnerability/wp-travel-engine/wordpress-wp-travel-engine-plugin-5-8-0-price- |

| 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** |
| | | | | | | manipulation-vulnerability?_s_id=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2024-5599 | **7.5** | FileOrganizer – Manage WordPress and Website Files plugin for WordPress | Sensitive Information Exposure | all versions up to, and including, 1.0.7 | N/A | https://wordpress.org/plugins/fileorganizer/<br>https://www.wordfence.com/threat-intel/vulnerabilities/id/78e7b65d-91f8-477e-b992-3148c1b65d7b?source=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2024-4887 | **7.5** | Qi Addons For Elementor plugin for WordPress | Remote File Inclusion | all versions up to, and including, 1.7.2 | N/A | https://wordpress.org/plugins/qi-addons-for-elementor/<br>https://www.wordfence.com/threat-intel/vulnerabilities/id/284daad9-d31e-4d29-ac15-ba293ba9640d?source=cve |
| https://nvd.nist.gov/vuln/detail/CVE-2024-5552 | **7.5** | kubeflow/kubeflow | Inefficient Regular Expression Complexity | N/A | N/A | https://github.com/kubeflow/kubeflow<br>https://huntr.com/bounties/0c1d6432-f385-4c54-beea-9f8c677def5b |
| https://nvd.nist.gov/vuln/detail/CVE-2023-4727 | **7.5** | dogtag-pki and pki-core | Authentication Bypass | N/A | N/A | https://www.dogtagpki.org/<br>https://bugzilla.redhat.com/show_bug.cgi?id=2232218 |

| 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-2024-26010 | **7.5** | Fortinet FortiPAM, FortiWeb, FortiAuthenticator, FortiSwitchManager, FortiOS, FortiProxy, | Stack-based Buffer Overflow | N/A | N/A | https://www.fortinet.com/products/fortipam<br>https://fortiguard.fortinet.com/psirt/FG-IR-24-036 |
| https://nvd.nist.gov/vuln/detail/CVE-2024-37130 | **7.3** | Dell OpenManage Server Administrator | Uncontrolled Search Path Element | 11.0.1.0 and prior | N/A | https://www.dell.com/support/kbdoc/en-us/000132087/support-for-dell-emc-openmanage-server-administrator-omsa<br>https://www.dell.com/support/kbdoc/en-us/000225914/dsa-2024-264-dell-openmanage-server-administrator-omsa-security-update-for-local-privilege-escalation-via-xsl-hijacking-vulnerability |

| **CISA/CERT-EU Alerts & Advisories** | | |
|---|---|---|
| **Σύντομη περιγραφή / Τίτλος** | **Αναγνωριστικό ευπάθειας** | **URL** |
| Microsoft Releases June 2024 Security Updates | Microsoft Security Update Guide for June | https://www.cisa.gov/news-events/alerts/2024/06/11/microsoft-releases-june-2024-security-updates |
| Fortinet Releases Security Updates for FortiOS | FG-IR-23-460: Multiple Buffer Overflows in Diag Npu Command | https://www.cisa.gov/news-events/alerts/2024/06/11/fortinet-releases-security-updates-fortios |
| CISA Releases Six Industrial Control Systems Advisories | ICSA-24-163-01 Rockwell Automation ControlLogix, GuardLogix, and CompactLogix<br>ICSA-24-163-02 AVEVA PI Web API<br>ICSA-24-163-03 AVEVA PI Asset Framework Client<br>ICSA-24-163-04 Intrado 911 Emergency Gateway<br>ICSA-23-108-02 Schneider Electric APC Easy UPS Online Monitoring Software (Update A)<br>ICSMA-24-163-01 MicroDicom DICOM Viewer<br>ICSA-24-158-01 Emerson PACSystem and Fanuc<br>ICSA-24-158-02 Emerson Ovation<br>ICSA-24-158-03 Mitsubishi Electric CC-Link IE TSN Industrial Managed Switch<br>ICSA-24-158-04 Johnson Controls Software House iStar Pro Door Controller | https://www.cisa.gov/news-events/alerts/2024/06/11/cisa-releases-six-industrial-control-systems-advisories<br>https://www.cisa.gov/news-events/alerts/2024/06/06/cisa-releases-four-industrial-control-systems-advisories |