Periodic newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 16/10/2024 - 23/10/2024

Contents

1 Common Vulnerabilities and Exposures (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-2024-45519	**10**	Zimbra Collaboration (ZCS)	allows unauthenticated users to execute commands	before 8.8.15 Patch 46, 9 before 9.0.0 Patch 41, 10 before 10.0.9, and 10.1 before 10.1.1	N/A	https://www.zimbra.com/ https://wiki.zimbra.com/wiki/Security_Center https://app.opencve.io/cve/CVE-2024-45519
https://nvd.nist.gov/vuln/detail/CVE-2024-9264	**9.9**	Grafana	Code Injection	N/A	N/A	https://grafana.com/ https://grafana.com/security/security-advisories/cve-2024-9264/
https://nvd.nist.gov/vuln/detail/CVE-2020-36837	**9.9**	ThemeGrill Demo Importer plugin for WordPress	Missing Authorization	1.3.4 through 1.6.1	N/A	https://wordpress.org/plugins/themegrill-demo-importer/ https://www.wordfence.com/threat-intel/vulnerabilities/id/8c0dc694-854e-4f96-8c2d-7251c41a3ee9?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-47575	**9.8**	**FortiManager (Also in CISA KEV database)**	**missing authentication for critical function**	**FortiManager 7.6.0, FortiManager 7.4.0 through 7.4.4, FortiManager 7.2.0 through 7.2.7, FortiManager 7.0.0 through 7.0.12, FortiManager 6.4.0 through 6.4.14, FortiManager 6.2.0 through 6.2.12, Fortinet FortiManager Cloud 7.4.1 through 7.4.4, FortiManager Cloud 7.2.1 through 7.2.7, FortiManager Cloud 7.0.1 through 7.0.13, FortiManager Cloud 6.4.1 through 6.4.7**	**N/A**	**https://fortimanager.forticloud.com/ https://fortiguard.fortinet.com/psirt/FG-IR-24-423**
https://nvd.nist.gov/vuln/detail/CVE-2024-44000	**9.8**	LiteSpeed Technologies LiteSpeed Cache	Insufficiently Protected Credentials	from n/a before 6.5.0.1	N/A	https://wordpress.org/plugins/litespeed-cache/ https://patchstack.com/database/vulnerability/litespeed-cache/wordpress-litespeed-cache-plugin-6-5-0-1-unauthenticated-account-takeover-vulnerability?_s_id=cve

https://nvd.nist.gov/vuln/detail/CVE-2024-9537	9.8	ScienceLogic SL1	Inclusion of Functionality from Untrusted Control Sphere	12.1.3+, 12.2.3+, and 12.3+	N/A	https://sciencelogic.com/platform/overview https://support.sciencelogic.com/s/article/15527
https://nvd.nist.gov/vuln/detail/CVE-2024-10119 https://debricked.com/vulnerability-database/vulnerability/CVE-2024-10118	9.8	SECOM (wireless router)	OS Command Injection	WRTM326 WRTR-304GN-304TW-UPSC	N/A	http://www.secom.com/ https://www.twcert.org.tw/en/cp-139-8157-e0461-2.html https://www.twcert.org.tw/tw/cp-132-8156-81c9d-1.html https://www.twcert.org.tw/en/cp-139-8155-c1ea6-2.html https://www.twcert.org.tw/tw/cp-132-8154-69fa5-1.html
https://nvd.nist.gov/vuln/detail/CVE-2024-43566	9.8	Microsoft Edge (Chromium-based)	Remote Code Execution	N/A	N/A	https://www.microsoft.com/en-us/edge/download https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43566
https://nvd.nist.gov/vuln/detail/CVE-2023-26785	9.8	MariaDB	Code Injection	N/A	N/A	https://mariadb.org/ https://github.com/Ant1sec-ops/CVE-2023-26785 https://seclists.org/fulldisclosure/2012/Dec/39
https://nvd.nist.gov/vuln/detail/CVE-2024-9863	9.8	UserPro plugin for WordPress	Incorrect Privilege Assignment	up to, and including, 3.6.0	N/A	https://codecanyon.net/item/userpro-user-profiles-with-social-login https://www.wordfence.com/threat-intel/vulnerabilities/id/f04eab14-dd86-4145-b5eb-20d064bc8417?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-9893	9.8	Nextend Social Login Pro plugin for WordPress	Authentication Bypass Using an Alternate Path or Channel	all versions up to, and including, 3.1.14	N/A	https://wordpress.org/plugins/nextend-facebook-connect/ https://www.wordfence.com/threat-intel/vulnerabilities/id/0e4588d1-f21e-48ba-a8cb-d18c421f000a?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-45216	9.8	Apache Solr	Improper Authentication	from 5.3.0 before 8.11.4, from 9.0.0 before 9.7.0	9.7.0, or 8.11.4	https://solr.apache.org/ https://solr.apache.org/security.html#cve-2024-45216-apache-solr-authentication-bypass-possible-using-a-fake-url-path-ending
https://nvd.nist.gov/vuln/detail/CVE-2021-4443	9.8	WordPress Mega Menu plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 2.0.6	N/A	https://wordpress.org/plugins/megamenu/ https://www.wordfence.com/threat-intel/vulnerabilities/id/04003542-fd62-4587-9834-70e7fe8f08ef?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2020-36832	9.8	Ultimate Membership Pro plugin for WordPress	Improper Authentication	between, and including, 7.3 to 8.6	N/A	https://codecanyon.net/item/ultimate-membership-pro-wordpress-plugin/12159253 https://www.wordfence.com/threat-intel/vulnerabilities/id/a5341bbd-55bd-41ad-b5d1-d6b56c141277?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2019-25217	9.8	SiteGround Optimizer plugin for WordPress	Missing Authorization	up to, and including, 5.0.12	N/A	https://wordpress.org/plugins/sg-cachepress/ https://www.wordfence.com/threat-intel/vulnerabilities/id/657f3bd7-2cdc-4eb6-ba50-7c7fca468df0?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2019-25213	9.8	Advanced Access Manager plugin for WordPress	Path Traversal	up to, and including, 5.9.8.1	N/A	https://wordpress.org/plugins/advanced-access-manager/ https://www.wordfence.com/threat-intel/vulnerabilities/id/55e0f0df-7be2-4e18-988c-2cc558768eff?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2018-25105	9.8	File Manager plugin for WordPress	Missing Authorization	up to, and including, 3.0	N/A	https://wordpress.org/plugins/wp-file-manager/ https://www.wordfence.com/threat-intel/vulnerabilities/id/a56d5a2f-ae13-4523-bc4a-17bb2fb4c6f0?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-9634	9.8	GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress	Deserialization of Untrusted Data	up to, and including, 3.16.3	N/A	https://wordpress.org/plugins/give/ https://www.wordfence.com/threat-intel/vulnerabilities/id/b8eb3aa9-fe60-48b6-aa24-7873dd68b47e?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-9486	9.8	Kubernetes (VM images built with Image Builder and Proxmox)	Use of Hard-coded Credentials	<= v0.1.37	N/A	https://github.com/kubernetes/kubernetes/issues/128006 https://github.com/kubernetes-sigs/image-builder/pull/1595 https://github.com/kubernetes/kubernetes/issues/128006
https://nvd.nist.gov/vuln/detail/CVE-2024-49195	9.8	Mbed TLS	Out-of-bounds Write	3.5.x through 3.6.x before 3.6.2	N/A	https://os.mbed.com/docs/mbed-os/v6.16/apis/tls.html https://mbed-tls.readthedocs.io/en/latest/tech-updates/security-advisories/
https://nvd.nist.gov/vuln/detail/CVE-2024-21216	9.8	Oracle WebLogic Server	Easily exploitable vulnerability	12.2.1.4.0 and 14.1.1.0.0	N/A	https://www.oracle.com/java/weblogic/ https://www.oracle.com/security-alerts/cpuoct2024.html
https://nvd.nist.gov/vuln/detail/CVE-2024-43698	9.8	Kieback & Peter's DDC4000	Use of Weak Credentials	N/A	N/A	https://www.kieback-peter.com/en/news/automation-system-ddc4000-meets-highest-bacnet-standards/ https://www.cisa.gov/news-events/ics-advisories/icsa-24-291-05
https://nvd.nist.gov/vuln/detail/CVE-2024-48904	9.8	Trend Micro Cloud Edge	execute arbitrary code	N/A	N/A	https://www.trendmicro.com/en_us/small-business/cloudedge-network-security.html https://success.trendmicro.com/en-US/solution/KA-0017998
https://nvd.nist.gov/vuln/detail/CVE-2024-47485	9.8	HikCentral Master Lite	CSV injection	N/A	N/A	https://www.hikvision.com/content/dam/hikvision/pt-br/data-sheets/HikCentral-Master-Lite-Datasheet_V1.0.0_20191120.pdf https://www.hikvision.com/en/support/cybersecurity/security-advisory/security-vulnerabilities-in-hikcentral-product-series/
https://nvd.nist.gov/vuln/detail/CVE-2024-49305	9.3	WPFactory Email Verification for WooCommerce	SQL Injection	from n/a through 2.8.10	N/A	https://wordpress.org/plugins/emails-verification-for-woocommerce/ https://patchstack.com/database/vulnerability/emails-verification-for-woocommerce/wordpress-customer-email-verification-for-woocommerce-plugin-2-8-10-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-49246	9.3	anand23 Ajax Rating	SQL Injection	from n/a through 1.1	N/A	https://wordpress.org/plugins/ajax-rating-with-custom-login/ https://patchstack.com/database/vulnerability/ajax-rating-with-custom-login/wordpress-ajax-rating-with-custom-login-plugin-1-1-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-37404	9.1	Ivanti Connect Secure	Improper Input Validation	before 22.7R2.1 and 9.1R18.9, or Ivanti Policy Secure before 22.7R1.1	N/A	https://www.ivanti.com/products/connect-secure-vpn https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-and-Policy-Secure-CVE-2024-37404
https://nvd.nist.gov/vuln/detail/CVE-2024-10025	9.1	SICK products	Use of Hard-coded Credentials	N/A	N/A	https://www.sick.com/at/en/ https://www.sick.com/.well-known/csaf/white/2024/sca-2024-0003.pdf
https://nvd.nist.gov/vuln/detail/CVE-2024-49271	9.1	Unlimited Elements Unlimited Elements For Elementor	Improper Neutralization of Special Elements	from n/a through 1.5.121.	N/A	https://wordpress.org/plugins/unlimited-elements-for-elementor/ https://patchstack.com/database/vulnerability/unlimited-elements-for-elementor/wordpress-unlimited-elements-for-elementor-free-widgets-addons-templates-plugin-1-5-121-remote-code-execution-rce-vulnerability?_s_id=cve

https://nvd.nist.gov/vuln/detail/CVE-2024-10004	9.1	Firefox for iOS	Improper Restriction of Rendered UI Layers or Frames	< 131.2	N/A	https://www.mozilla.org/en-US/firefox/browsers/mobile/ios/ https://www.mozilla.org/security/advisories/mfsa2024-54/
https://nvd.nist.gov/vuln/detail/CVE-2024-21172	9	Oracle Hospitality OPERA	Difficult to exploit vulnerability	5.6.19.19, 5.6.25.8 and 5.6.26.4	N/A	https://www.oracle.com/hospitality/products/opera-property-services/ https://www.oracle.com/security-alerts/cpuoct2024.html
https://nvd.nist.gov/vuln/detail/CVE-2024-38124	9	Windows Netlogon	Elevation of Privilege	Windows Server 2008 Windows Server 2008 R2 Windows Server 2008 Sp2 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019 Windows Server 2022 Windows Server 2022 23h2 Windows Server 23h2	N/A	https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-nrpc/ff8f970f-3e37-40f7-bd4b-af7336e4792f https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38124
https://nvd.nist.gov/vuln/detail/CVE-2024-10194	8.8	WAVLINK routers	Stack-based Buffer Overflow	WN530H4, WN530HG4 and WN572HG3 up to 20221028	N/A	https://www.wavlink.com/en_us/index.html https://docs.google.com/document/d/1PodIMRe1f0Ql83jUXV5VIoc-Xsf9VC1K
https://nvd.nist.gov/vuln/detail/CVE-2024-10130	8.8	Tenda AC8	Stack-based Buffer Overflow	16.03.34.06	N/A	https://www.tendacn.com/product/overview/ac8.html https://github.com/JohenanLi/router_vuls/blob/main/ac8v4/FUN_004a8838.md
https://nvd.nist.gov/vuln/detail/CVE-2024-38814	8.8	VMware HCX	SQL Injection	N/A	N/A	https://www.vmware.com/products/cloud-infrastructure/hcx https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25019
https://nvd.nist.gov/vuln/detail/CVE-2024-45711	8.8	SolarWinds Serv-U	Path Traversal	N/A	N/A	https://www.solarwinds.com/serv-u-managed-file-transfer-server https://www.solarwinds.com/trust-center/security-advisories/CVE-2024-45711
https://nvd.nist.gov/vuln/detail/CVE-2024-45693	8.8	Apache CloudStack	Cross-Site Request	4.15.1.0 through 4.18.2.3 and 4.19.0.0 through 4.19.1.1	4.18.2.4 or 4.19.1.2, or later	https://cloudstack.apache.org/ https://cloudstack.apache.org/blog/security-release-advisory-4.18.2.4-4.19.1.2

			Forgery (CSRF)			
https://nvd.nist.gov/vuln/detail/CVE-2021-4450	8.8	Post Grid plugin for WordPress	SQL Injection	up to, and including, 2.1.12	N/A	https://wordpress.org/plugins/post-grid/ https://www.wordfence.com/threat-intel/vulnerabilities/id/a321b112-ce37-4a0e-800f-f3feef6ac799?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2021-4447	8.8	Essential Addons for Elementor plugin for WordPress	Missing Authorization	up to and including 4.6.4	N/A	https://wordpress.org/plugins/essential-addons-for-elementor-lite/ https://www.wordfence.com/threat-intel/vulnerabilities/id/be098ee9-b749-4908-85e8-e717d019609a?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-21254	8.8	Oracle BI Publisher	Easily exploitable vulnerability	7.0.0.0.0, 7.6.0.0.0 and 12.2.1.4.0	N/A	https://www.oracle.com/middleware/technologies/analytics-publisher.html https://www.oracle.com/security-alerts/cpuoct2024.html
https://nvd.nist.gov/vuln/detail/CVE-2024-38212	8.8	Windows Routing and Remote Access Service (RRAS)	Remote Code Execution	Windows Server 2008 Windows Server 2008 R2 Windows Server 2008 Sp2 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019 Windows Server 2022 Windows Server 2022 23h2 Windows Server 23h2	N/A	https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn614140(v=ws.11) https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38212
https://nvd.nist.gov/vuln/detail/CVE-2024-6380	8.7	3DEXPERIENCE R2022x	Cross-site Scripting	N/A	N/A	https://events.3ds.com/3dexperience-2022 https://www.3ds.com/vulnerability/advisories
https://nvd.nist.gov/vuln/detail/CVE-2024-49297	8.5	Zoho CRM Lead Magnet	SQL Injection	from n/a through 1.7.9.0	N/A	https://wordpress.org/plugins/zoho-crm-forms/ https://patchstack.com/database/vulnerability/zoho-crm-forms/wordpress-zoho-crm-lead-magnet-plugin-1-7-9-0-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-49244	8.5	CSV Product Import Export for WooCommerce	SQL Injection	from n/a through 1.0.0	N/A	https://wordpress.org/plugins/product-import-export-for-woo/ https://patchstack.com/database/vulnerability/csv-wc-product-import-export/wordpress-sv-product-import-export-for-woocommerce-plugin-1-0-0-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-47304	8.5	WPManageNinja LLC Fluent Support	SQL Injection	from n/a through 1.8.0	N/A	https://wordpress.org/plugins/fluent-support/ https://patchstack.com/database/vulnerability/fluent-support/wordpress-fluent-support-plugin-1-8-0-sql-injection-vulnerability?_s_id=cve

https://nvd.nist.gov/vuln/detail/CVE-2024-7755	8.2	EWON FLEXY 202	Insufficiently Protected Credentials	N/A	N/A	https://www.hms-networks.com/p/flexy20200-00ma-ewon-flexy-202 https://www.cisa.gov/news-events/ics-advisories/icsa-24-291-04
https://nvd.nist.gov/vuln/detail/CVE-2024-20458	8.2	Cisco ATA 190 Series Analog Telephone Adapter	OS Command Injection	N/A	N/A	https://www.cisco.com/c/en/us/products/unified-communications/ata-190-series-analog-telephone-adapters/index.html https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multi-RDTEqRsy
https://nvd.nist.gov/vuln/detail/CVE-2024-49579	8.1	JetBrains YouTrack	Improper Verification of Source	before 2024.3.47197	N/A	https://www.jetbrains.com/youtrack/ https://www.jetbrains.com/privacy-security/issues-fixed/
https://nvd.nist.gov/vuln/detail/CVE-2024-21252	8.1	Oracle Product Hub	Easily exploitable vulnerability	12.2.3-12.2.13	N/A	https://www.oracle.com/webfolder/s/quicktours/scm/gqt-scm-pmdm-overview/index.html https://www.oracle.com/security-alerts/cpuoct2024.html
https://nvd.nist.gov/vuln/detail/CVE-2024-48637	8	D-Link DIR_882_FW130B06 and DIR_878 DIR_878_FW130B08	OS Command Injection	N/A	N/A	https://www.dlink.com/gr/el/products/dir-882-exo-ac2600-mumimo-wifi-router https://www.dlink.com/en/security-bulletin/
https://nvd.nist.gov/vuln/detail/CVE-2024-48192	8	Tenda G3	Use of Hard-coded Credentials	v15.01.0.5(2848_755) _EN	N/A	https://www.tendacn.com/product/g3.html https://colorful-meadow-5b9.notion.site/G3_HardCode_vuln-6b5ae19473b745d7abe5e01b4529caf8?pvs=4
https://nvd.nist.gov/vuln/detail/CVE-2024-45766	8	Dell OpenManage Enterprise	Code Injection	4.1 and prior	N/A	https://www.dell.com/en-us/lp/dt/open-manage-enterprise https://www.dell.com/support/kbdoc/en-us/000237300/dsa-2024-426-security-update-for-dell-openmanage-enterprise-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2024-29821	7.8	Ivanti DSM	insecure ACLs	< version 2024.2	N/A	https://forums.ivanti.com/s/desktop-and-server-management-dsm?language=en_US https://forums.ivanti.com/s/article/SA-2024-07-12-CVE-2024-29821
https://nvd.nist.gov/vuln/detail/CVE-2024-10068	7.8	OpenSight Software FlashFXP	Uncontrolled Search Path Element	5.4.0.3970	N/A	https://www.flashfxp.com/ https://vuldb.com/?ctiid.280716 https://vuldb.com/?id.280716 https://vuldb.com/?submit.419684
https://nvd.nist.gov/vuln/detail/CVE-2024-49389	7.8	Acronis Cyber Files (Windows)	Incorrect Default Permissions	before build 9.0.0x24	N/A	https://www.acronis.com/en-us/support/mobility/files-advanced/ https://security-advisory.acronis.com/advisories/SEC-5319
https://nvd.nist.gov/vuln/detail/CVE-2024-9858	7.8	Google Cloud Migrate	Incorrect Default Permissions	from version 1.1.0 to 1.2.2 Windows installs	N/A	https://cloud.google.com/products/cloud-migration https://cloud.google.com/migrate/containers/docs/m2c-cli-relnotes#october_8_2024
https://nvd.nist.gov/vuln/detail/CVE-2024-49215	7.8	Sangoma Asterisk	path traversal	through 18.20.0, 19.x and 20.x through 20.5.0, and 21.x through 21.0.0	N/A	https://sangoma.com/products-and-solutions/open-source/ https://github.com/asterisk/asterisk/blob/20.5.0/main/manager.c#L3755
https://nvd.nist.gov/vuln/detail/CVE-2024-48903	7.8	Trend Micro Deep Security Agent 20	improper access control	N/A	N/A	https://www.trendmicro.com/en_us/business/products/hybrid-cloud/deep-security.html https://success.trendmicro.com/en-US/solution/KA-0017997

https://nvd.nist.gov/vuln/detail/CVE-2024-47522	7.7	Suricata	Reachable Assertion	N/A	7.0.7	https://suricata.io/ https://github.com/OISF/suricata/security/advisories/GHSA-w5xv-6586-jpm7
https://nvd.nist.gov/vuln/detail/CVE-2024-21536	7.5	http-proxy-middleware	Uncontrolled Resource Consumption	before 2.0.7, from 3.0.0 and before 3.0.3	N/A	https://www.npmjs.com/package/http-proxy-middleware https://security.snyk.io/vuln/SNYK-JS-HTTPPROXYMIDDLEWARE-8229906
https://nvd.nist.gov/vuln/detail/CVE-2024-4740	7.5	MXsecurity software	Use of Hard-coded Credentials	v1.1.0 and prior	N/A	https://www.moxa.com/en/products/industrial-network-infrastructure/network-management-software/mxsecurity-series https://www.moxa.com/en/support/product-support/security-advisory/mpsa-231878-mxsecurity-series-multiple-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2024-10173	7.3	didi DDMQ (distributed messaging product)	Improper Authentication	1	N/A	https://github.com/didi/DDMQ https://github.com/didi/DDMQ/issues/37#issue-2577905007
https://nvd.nist.gov/vuln/detail/CVE-2023-6729	7.3	Nokia SR OS routers	Incorrect Permission Assignment for Critical Resource	N/A	N/A	https://www.nokia.com/networks/ip-networks/service-router-operating-system-nos/ https://www.nokia.com/about-us/security-and-privacy/product-security-advisory/cve-2023-6729/
https://nvd.nist.gov/vuln/detail/CVE-2024-6333	7.2	Altalink, Versalink & WorkCentre Product	Improper Input Validation	N/A	N/A	https://download.support.xerox.com/pub/docs/ALB81XX/userdocs/any-os/ar/D7.8_AltaLink_VersaLink_Product_Enhancements_Read_Me_04600v2.pdf https://securitydocs.business.xerox.com/wp-content/uploads/2024/10/Xerox-Security-Bulletin-XRX24-015-for-Altalink-Versalink-and-WorkCentre-%E2%80%93-CVE-2024-6333-.pdf
https://nvd.nist.gov/vuln/detail/CVE-2024-45844	7.2	BIG-IP monitor functionality (Software versions which have reached End of Technical Support (EoTS) are not evaluated)	Missing Authentication for Critical Function	N/A	N/A	https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-monitors-reference-12-0-0/2.html https://my.f5.com/manage/s/article/K000140061
https://nvd.nist.gov/vuln/detail/CVE-2024-44061	7.1	WPFactory EU/UK VAT Manager for WooCommerce	Basic XSS	from n/a through 2.12.14	N/A	https://wordpress.org/plugins/eu-vat-for-woocommerce/ https://patchstack.com/database/vulnerability/eu-vat-for-woocommerce/wordpress-eu-uk-vat-manager-for-woocommerce-plugin-2-12-8-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-30875	7.1	JavaScript Library jquery-ui	Cross-site Scripting	v.1.13.1	N/A	https://jqueryui.com/ https://github.com/Ant1sec-ops/CVE-2024-30875

2 CISA/CERT-EU Alerts & Advisories

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	**Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες**	**URL**
CISA Releases Industrial Control Systems Advisory	ICSA-24-296-01 ICONICS and Mitsubishi Electric Products ICSA-24-291-01 Elvaco M-Bus Metering Gateway CMe3100 ICSA-24-291-02 LCDS LAquis SCADA ICSA-24-291-03 Mitsubishi Electric CNC Series ICSA-24-291-04 HMS Networks EWON FLEXY 202 ICSA-24-291-05 Kieback&Peter DDC4000 Series ICSA-24-270-04 goTenna Pro X and Pro X2 (Update A) ICSA-24-270-05 goTenna Pro ATAK Plugin (Update A)	https://www.cisa.gov/news-events/alerts/2024/10/22/cisa-releases-one-industrial-control-systems-advisory https://www.cisa.gov/news-events/alerts/2024/10/17/cisa-releases-seven-industrial-control-systems-advisories
CISA Adds Known Exploited Vulnerability to Catalog	CVE-2024-38094 Microsoft SharePoint Deserialization Vulnerability CVE-2024-9537 ScienceLogic SL1 Unspecified Vulnerability CVE-2024-40711 Veeam Backup and Replication Deserialization Vulnerability **CVE-2024-47575 Fortinet FortiManager Missing Authentication Vulnerability**	https://www.cisa.gov/news-events/alerts/2024/10/22/cisa-adds-one-known-exploited-vulnerability-catalog https://www.cisa.gov/news-events/alerts/2024/10/21/cisa-adds-one-known-exploited-vulnerability-catalog https://www.cisa.gov/news-events/alerts/2024/10/17/cisa-adds-one-known-exploited-vulnerability-catalog **https://www.cisa.gov/news-events/alerts/2024/10/23/cisa-adds-one-known-exploited-vulnerability-catalog**
Oracle Releases Quarterly Critical Patch Update Advisory for October 2024	Oracle Critical Patch Update Advisory – October 2024	https://www.cisa.gov/news-events/alerts/2024/10/17/oracle-releases-quarterly-critical-patch-update-advisory-october-2024
CISA, FBI, NSA, and International Partners Release Advisory on Iranian Cyber Actors Targeting Critical Infrastructure Organizations Using Brute Force	Cybersecurity Advisory	https://www.cisa.gov/news-events/alerts/2024/10/16/cisa-fbi-nsa-and-international-partners-release-advisory-iranian-cyber-actors-targeting-critical

3 News

News	
Σύντομη περιγραφή / Τίτλος	**URL**
CISA proposes new security requirements to protect govt, personal data	https://www.bleepingcomputer.com/news/security/cisa-proposes-new-security-requirements-to-protect-govt-personal-data/
Cyberattack Targets Critical Sectors in Cyprus	https://dailysecurityreview.com/security-spotlight/cyberattack-targets-critical-sectors-in-cyprus/
Cyprus Successfully Defends Against Wave of DDoS Cyberattacks	https://dailysecurityreview.com/security-spotlight/cyprus-successfully-defends-against-wave-of-ddos-cyberattacks/
VMware fixes bad patch for critical vCenter Server RCE flaw	https://www.bleepingcomputer.com/news/security/vmware-fixes-bad-patch-for-critical-vcenter-server-rce-flaw/
SecureWorks to be acquired by Sophos for $859M	https://www.scworld.com/brief/secureworks-to-be-acquired-by-sophos-for-859m
VMware failed to fully address vCenter Server RCE flaw CVE-2024-38812	https://securityaffairs.com/170096/security/vmware-failed-to-fix-rce-vcenter-server-cve-2024-38812.html
Internet Archive (Archive.org) Hacked for Second Time in a Month	https://hackread.com/internet-archive-archive-org-hacked-for-second-time/
Akira ransomware continues to evolve	https://blog.talosintelligence.com/akira-ransomware-continues-to-evolve/
Week in review: 87k+ Fortinet devices still open to attack, red teaming tool used for EDR evasion	https://www.helpnetsecurity.com/2024/10/20/week-in-review-87k-fortinet-devices-still-open-to-attack-red-teaming-tool-used-for-edr-evasion/

3.1 Breaches

News - Breaches	
Σύντομη περιγραφή / Τίτλος	**URL**
Largest Retail Breach in History: 350 Million “Hot Topic” Customers’ Personal & Payment Data Exposed — As a Result of Infostealer Infection	https://www.infostealers.com/article/largest-retail-breach-in-history-350-million-hot-topic-customers-personal-and-payment-data-exposed-as-a-result-of-infostealer-infection/
Transak Hit by Data Breach: 57,000 Users Affected by Stormous Ransomware Attack	https://dailysecurityreview.com/security-spotlight/transak-hit-by-data-breach-57000-users-affected-by-stormous-ransomware-attack/
AWS, Azure auth keys found in Android and iOS apps used by millions	https://www.bleepingcomputer.com/news/security/aws-azure-auth-keys-found-in-android-and-ios-apps-used-by-millions/
Cisco Confirms Data Breach: Public-Facing DevHub Targeted by Hackers	https://dailysecurityreview.com/security-spotlight/cisco-confirms-data-breach-public-facing-devhub-targeted-by-hackers/
Cisco Disables DevHub Access After Security Breach	https://www.darkreading.com/cloud-security/cisco-disables-access-devhub-site-security-breach
50,000 Files Exposed in Nidec Ransomware Attack	https://www.infosecurity-magazine.com/news/nidec-ransomware-attack-expose/

3.2 Vulnerabilities and flaws

News – Vulnerabilities and Flaws	
Σύντομη περιγραφή / Τίτλος	**URL**
Samsung Zero-Day Vuln Under Active Exploit, Google Warns	https://www.darkreading.com/endpoint-security/samsung-zero-day-vuln-under-active-exploit-google-warns
OPA for Windows Vulnerability Exposes NTLM Hashes	https://www.darkreading.com/vulnerabilities-threats/opa-windows-vulnerability-exposes-ntlm-hashes
Roundcube XSS flaw exploited to steal credentials, email (CVE-2024-37383)	https://www.helpnetsecurity.com/2024/10/22/cve-2024-37383-exploited/
Fortinet releases patches for undisclosed critical FortiManager vulnerability	https://www.helpnetsecurity.com/2024/10/21/fortimanager-critical-vulnerability/
High-Risk Vulnerabilities in Apache HTTP Server's mod_proxy Encoding Problem Allow Authentication Bypass — $$$ Bounty	https://infosecwriteups.com/high-risk-vulnerabilities-in-apache-http-servers-mod-proxy-encoding-problem-allow-authentication-cbe8d422738d

3.3 Potential threats / Threat intelligence

News – Potential Threats / Threat Intelligence	
Σύντομη περιγραφή / Τίτλος	**URL**
Ransomware Gangs Use LockBit's Fame to Intimidate Victims in Latest Attacks	https://thehackernews.com/2024/10/ransomware-gangs-use-lockbits-fame-to.html
US Energy Sector Vulnerable to Supply Chain Attacks	https://www.infosecurity-magazine.com/news/us-energy-vulnerable-supply-chain/
Bumblebee malware infection chain seen for the first time since May	https://www.scworld.com/news/bumblebee-malware-infection-chain-seen-for-the-first-time-since-may
Swarms of Fake WordPress Plug-ins Infect Sites With Infostealers	https://www.darkreading.com/endpoint-security/swarms-fake-wordpress-plug-ins-infect-sites-infostealers
Fake CAPTCHA Pages Used by Lumma Stealer to Spread Fileless Malware	https://hackread.com/fake-captcha-pages-lumma-stealer-fileless-malware/
Gambling sector subjected to APT41 intrusions	https://www.scworld.com/brief/gambling-sector-subjected-to-apt41-intrusions
Experts warn of a new wave of Bumblebee malware attacks	https://securityaffairs.com/170112/malware/bumblebee-malware-attacks.html
Russia subjected to intrusions with LockBit 3.0, Babuk ransomware	https://www.scworld.com/brief/russia-subjected-to-intrusions-with-lockbit-3-0-babuk-ransomware
Mirai-Inspired Gorilla Botnet Hits 0.3 Million Targets Across 100 Countries	https://hackread.com/mira-gorilla-botnet-ddos-attacks-hit-100-countries/

3.4 Guides / Tools

News – Guides / Tools	
Σύντομη περιγραφή / Τίτλος	**URL**
Argus: Open-source information gathering toolkit	https://www.helpnetsecurity.com/2024/10/23/argus-open-source-information-gathering-toolkit/
Honeypots 104: T-Pot — Your All-in-One Honeypot Platform Guide	https://infosecwriteups.com/honeypots-104-t-pot-your-all-in-one-honeypot-platform-guide-0ba2643bc597
APTs: Tactics, Techniques, and Procedures	https://infosecwriteups.com/apts-tactics-techniques-and-procedures-b306f91dc374
Social Engineering Attacks: How to Spot and Prevent Scams	https://medium.com/@thecompany323/social-engineering-attacks-how-to-spot-and-prevent-scams-64b8ca12a6de

4 References

[1]. Ο βαθμός επικινδυνότητας είναι σύμφωνα με την κλίμακα Common Vulnerability Scoring System (CVSSv3), https://nvd.nist.gov/vuln-metrics/cvss

[2]. Τα CVEs αποτελέσματα που εμφανίζονται στην ενότητα 1 διαθέτουν CVSSv3 score >= 7.0 και έχει γίνει μια επιλογή συστημάτων/υπηρεσιών ανάλογα με το πόσο διαδεδομένα είναι.

[3]. Τα CVEs που αφορούν Wordpress plugins θα εμφανίζονται σε ξεχωριστή ενότητα (1.1) σε περιόδους που η εμφάνισή τους είναι ιδιαίτερα αυξημένη.