Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 24/10/2024 - 30/10/2024

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-2024-45656	9.8	IBM Flexible Service Processor	Use of Hard-coded Credentials	FW860.00 through FW860.B3, FW950.00 through FW950.C0, FW1030.00 through FW1030.61, FW1050.00 through FW1050.21, and FW1060.00 through FW1060.10	N/A	https://community.ibm.com/community/user/power/blogs/ratan-gupta1/2020/06/11/power-systems-flexible-service-processor-fsp-secur https://www.ibm.com/support/pages/node/7174183
https://nvd.nist.gov/vuln/detail/CVE-2024-20424	9.9	Cisco Secure Firewall Management Center	OS Command Injection	N/A	N/A	https://www.cisco.com/site/us/en/products/security/firewalls/firewall-management-center/index.html https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-cmd-inj-v3AWDqN7
https://nvd.nist.gov/vuln/detail/CVE-2024-9501	9.8	Wp Social Login and Register Social Counter plugin for WordPress	Authentication Bypass	all versions up to, and including, 3.0.7	N/A	https://wordpress.org/plugins/wp-social/ https://www.wordfence.com/threat-intel/vulnerabilities/id/a4294f5f-d989-4b97-88ee-4e94f4f7845a?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-10386	9.8	Rockwell Automation devices	Missing Authentication for Critical Function	N/A	N/A	https://www.rockwellautomation.com/en-us.html https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1708.html
https://nvd.nist.gov/vuln/detail/CVE-2022-30357	9.8	OvalEdge	Cross-Site Request Forgery (CSRF)	5.2.8.0	N/A	https://www.ovaledge.com/ https://cve.offsecguy.com/ovaledge/vulnerabilities/account-takeover#cve-2022-30357
https://nvd.nist.gov/vuln/detail/CVE-2024-9488	9.8	Comments – wpDiscuz plugin for WordPress	Authentication Bypass	all versions up to, and including, 7.6.24	N/A	https://wordpress.org/plugins/wpdiscuz/ https://www.wordfence.com/threat-intel/vulnerabilities/id/b71706a7-e101-4d50-a2da-1aeeaf07cf4b?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-7763	9.8	WhatsUp Gold	Improper Authentication	before 2024.0.0	N/A	https://www.whatsupgold.com/ https://community.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-August-2024 https://www.progress.com/network-monitoring
https://nvd.nist.gov/vuln/detail/CVE-2024-8923	9.8	AI with the Now Platform	Code Injection	N/A	N/A	https://www.servicenow.com/now-platform.html https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1706070

https://nvd.nist.gov/vuln/detail/CVE-2024-10468 https://nvd.nist.gov/vuln/detail/CVE-2024-10467	9.8	IndexedDB API (Mozilla)	Allocation of Resources Without Limits or Throttling Classic Buffer Overflow	Firefox < 132 and Thunderbird < 132 Firefox 131, Firefox ESR 128.3, and Thunderbird 128.3	N/A	https://developer.mozilla.org/en-US/docs/Web/API/IndexedDB_API https://www.mozilla.org/security/advisories/mfsa2024-55/ https://www.mozilla.org/security/advisories/mfsa2024-59/ https://www.mozilla.org/security/advisories/mfsa2024-56/ https://www.mozilla.org/security/advisories/mfsa2024-58/
https://nvd.nist.gov/vuln/detail/CVE-2024-20412	9.3	Cisco Firepower Threat Defense	Use of Hard-coded Password	Cisco Firepower 1000, 2100, 3100, and 4200 Series	N/A	https://www.cisco.com/c/en/us/support/security/firepower-ngfw/series.html https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-statcred-dFC8tXT5
https://nvd.nist.gov/vuln/detail/CVE-2024-38821	9.1	Spring WebFlux applications	Allocation of Resources Without Limits or Throttling	N/A	N/A	https://docs.spring.io/spring-boot/reference/web/reactive.html https://spring.io/security/cve-2024-38821
https://nvd.nist.gov/vuln/detail/CVE-2024-47821	9.1	pyLoad (free and open-source Download Manager)	remote code execution	N/A	N/A	https://pyload.net/ https://github.com/pyload/pyload/security/advisories/GHSA-w7hq-f2pj-c53g
https://nvd.nist.gov/vuln/detail/CVE-2024-47406	9.1	Sharp and Toshiba Tec MFPs	Authentication Bypass	N/A	N/A	https://www.toshibatec.eu/products/multifunctional-systems-and-printers/e-studio509cs/ https://global.sharp/products/copier/info/info_security_2024-10.html
https://nvd.nist.gov/vuln/detail/CVE-2024-48145	9.1	Netangular Technologies ChatNet AI	Command Injection	v1.0	N/A	https://netangular.com/ https://github.com/soursec/CVEs/tree/main/CVE-2024-48145
https://nvd.nist.gov/vuln/detail/CVE-2024-48144	9.1	Fusion Chat Chat AI Assistant Ask Me Anything	Command Injection	v1.2.4.0	N/A	https://fusionchat.ai/ https://github.com/soursec/CVEs/tree/main/CVE-2024-48144
https://nvd.nist.gov/vuln/detail/CVE-2024-48143	9.1	Digitory Multi Channel Integrated POS	Improper Restriction of Excessive Authentication Attempts	v1.0	N/A	https://digitory.com/multi-channel-integrated-pos/ https://github.com/soursec/CVEs/tree/main/CVE-2024-48143
https://nvd.nist.gov/vuln/detail/CVE-2024-47883	9.1	OpenRefine fork of the MIT Simile Butterfly server	Absolute Path Traversal	N/A	N/A	https://openrefine.org/ https://github.com/OpenRefine/simile-butterfly/security/advisories/GHSA-3p8v-w8mr-m3x8
https://nvd.nist.gov/vuln/detail/CVE-2024-7474	9.1	lunary-ai/lunary	Improper Access Control	1.3.2	N/A	https://lunary.ai/ https://github.com/lunary-ai/lunary/commit/8f563c77d8614a72980113f530c7a9ec15a5f8d5
https://nvd.nist.gov/vuln/detail/CVE-2024-42028	8.8	Self-Hosted UniFi Network Server	Incorrect Default Permissions	Version 8.4.62 and earlier)	N/A	https://help.ui.com/hc/en-us/articles/360012282453-Self-Hosting-a-UniFi-Network-Server https://community.ui.com/releases/Security-Advisory-Bulletin-043-043/28e45c75-314e-4f07-a4f3-d17f67bd53f7

https://nvd.nist.gov/vuln/detail/CVE-2024-10434	8.8	Tenda AC1206	Stack-based Buffer Overflow	up to 20241027	N/A	https://www.tendacn.com/gr/product/ac6v5.html https://github.com/physicszq/Routers/blob/main/Tenda/README.md
https://nvd.nist.gov/vuln/detail/CVE-2024-9598	8.8	AMP for WP – Accelerated Mobile Pages plugin for WordPress	Cross-Site Request Forgery (CSRF)	all versions up to, and including, 1.0.99.1	N/A	https://wordpress.org/plugins/accelerated-mobile-pages/ https://www.wordfence.com/threat-intel/vulnerabilities/id/6b155ec8-d69d-40cf-8bea-201629bc9ca6?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-10351	8.8	Tenda RX9 Pro	Stack-based Buffer Overflow	22.03.02.20	N/A	https://www.tendacn.com/product/overview/rx9pro.html https://gitee.com/GXB0_0/iot-vul/blob/master/Tenda/RX9/20/setMacFilterCfg.md
https://nvd.nist.gov/vuln/detail/CVE-2024-45263	8.8	GL-iNet devices	Unrestricted Upload of File with Dangerous Type	MT6000, MT3000, MT2500, AXT1800, and AX1800 4.6.2	N/A	https://www.gl-inet.com/products/ https://github.com/gl-inet/CVE-issues/blob/main/4.0.0/Arbitrary%20File%20Upload%20to%20ovpn_upload%20via%20Upload%20Interface.md
https://nvd.nist.gov/vuln/detail/CVE-2024-48441	8.8	Tianyu CPE Router CommonCPExCPETS_v3.2.468.11.04_P4	Command Injection	CommonCPExCPETS_v3.2.468.11.04_P4	N/A	https://www.whtyglobal.com/ https://medium.com/%40sengkyaut/unauthenticated-factory-mode-reset-and-at-command-injection-in-jboneos-or-jbonecloud-firmware-1dec156b7ddd
https://nvd.nist.gov/vuln/detail/CVE-2024-48440	8.8	CPE Router NR500-EA RG500UEAABxCOMSLICv3.2.2543.12.18	Command Injection	NR500-EA RG500UEAABxCOMSLICv3.2.2543.12.18	N/A	https://github.com/advisories/GHSA-m584-rmpj-6q5p https://medium.com/%40sengkyaut/unauthenticated-factory-mode-reset-and-at-command-injection-in-jboneos-or-jbonecloud-firmware-1dec156b7ddd
https://nvd.nist.gov/vuln/detail/CVE-2024-40431	8.8	Realtek SD card reader	lack of input validation	before 10.0.26100.21374	N/A	https://www.realtek.com/Download/List?cate_id=590&menu_id=405 https://zwclose.github.io/2024/10/14/rtsper1.html
https://nvd.nist.gov/vuln/detail/CVE-2024-8312	8.7	GitLab CE/EE	Cross-site Scripting	ersions from 15.10 before 17.3.6, 17.4 before 17.4.3, and 17.5 before 17.5.1	N/A	https://about.gitlab.com/install/ce-or-ee/ https://gitlab.com/gitlab-org/gitlab/-/issues/481819
https://nvd.nist.gov/vuln/detail/CVE-2024-48208	8.6	pure-ftpd	Out-of-bounds Read	before 1.0.52	N/A	https://www.pureftpd.org/project/pure-ftpd/ https://github.com/jedisct1/pure-ftpd/pull/176
https://nvd.nist.gov/vuln/detail/CVE-2024-20495	8.6	Remote Access VPN feature of Cisco Adaptive Security Appliance (ASA)	Improper Input Validation	N/A	N/A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-vpn-cZf8gT
https://nvd.nist.gov/vuln/detail/CVE-2024-5608	8.3	Zohocorp ManageEngine ADAudit Plus	SQL Injection	below 8121	N/A	https://www.manageengine.com/products/active-directory-audit/sem/lp/active-directory-auditing.html https://www.manageengine.com/products/active-directory-audit/cve-2024-5608.html
https://nvd.nist.gov/vuln/detail/CVE-2024-0126	8.2	NVIDIA GPU Display Driver for Windows and Linux	Improper Input Validation	N/A	N/A	https://docs.nvidia.com/vgpu/index.html https://nvidia.custhelp.com/app/answers/detail/a_id/5586
https://nvd.nist.gov/vuln/detail/CVE-2024-44100 https://nvd.nist.gov/vuln/detail/CVE-2024-47031 https://nvd.nist.gov/vuln/detail/CVE-2024-47023	8.1	Android system (special reference to Google pixel devices)	information disclosure	before 2024-10-05	N/A	https://source.android.com/docs/security/bulletin/2024-10-01 https://source.android.com/security/bulletin/pixel/2024-10-01

https://nvd.nist.gov/vuln/detail/CVE-2024-10011	8.1	BuddyPress plugin for WordPress	Path Traversal	all versions up to, and including, 14.1.0	N/A	https://wordpress.org/plugins/buddypress/ https://www.wordfence.com/threat-intel/vulnerabilities/id/4327f414-64f4-4193-a5c0-2a5ecdd75e11?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-10327	8.1	Okta Verify for iOS	Improper Authentication	versions 9.25.1 (beta) and 9.27.0 (including beta)	N/A	https://apps.apple.com/us/app/okta-verify/id490179405 https://trust.okta.com/security-advisories/okta-verify-for-ios-cve-2024-10327/
https://nvd.nist.gov/vuln/detail/CVE-2024-10313	8	iniNet Solutions SpiderControl SCADA PC HMI Editor	Path Traversal	N/A	N/A	https://spidercontrol.net/spidercontrol-products/a-design-tool-hmi-editor/?lang=en https://www.cisa.gov/news-events/ics-advisories/icsa-24-298-02
https://nvd.nist.gov/vuln/detail/CVE-2024-45242	7.8	EnGenius ENH1350EXT	OS Command Injection	through 3.9.3.2_c1.9.51	N/A	https://www.engeniustech.com/eu/products/wireless/outdoor-access-points/enh1350ext/ https://github.com/actuator/cve/blob/main/Engenius/CVE-2024-45242_Extended_Report.pdf
https://nvd.nist.gov/vuln/detail/CVE-2024-45802	7.5	Squid	Improper Input Validation	N/A	N/A	https://www.squid-cache.org/ https://github.com/squid-cache/squid/security/advisories/GHSA-f975-v7qw-q7hj
https://nvd.nist.gov/vuln/detail/CVE-2024-10455	7.5	BPv7 parser in µD3TN	Reachable Assertion	v0.14.0	N/A	https://d3tn.com/ud3tn.html https://gitlab.com/d3tn/ud3tn/-/issues/227
https://nvd.nist.gov/vuln/detail/CVE-2024-10402	7.5	Forminator Forms – Contact Form, Payment Form & Custom Form Builder plugin for WordPress	Missing Authorization	all versions up to, and including, 1.35.1	N/A	https://wordpress.org/plugins/forminator/ https://www.wordfence.com/threat-intel/vulnerabilities/id/be1d9d2b-cbdf-4d62-85fe-2616eaf02848?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-49757	7.5	Zitadel	Improper Authentication	prior to 2.63.4	N/A	https://zitadel.com/ https://github.com/zitadel/zitadel/security/advisories/GHSA-3rmw-76m6-4gjc
https://nvd.nist.gov/vuln/detail/CVE-2024-49359	7.5	ZimaOS	Files or Directories Accessible to External Parties	1.2.4 and all prior versions	N/A	https://github.com/IceWhaleTech/ZimaOS https://github.com/IceWhaleTech/ZimaOS/security/advisories/GHSA-mwpw-fhrm-728x
https://nvd.nist.gov/vuln/detail/CVE-2024-48140	7.5	Butterfly Effect Limited Monica Your AI Copilot	Command Injection	v6.3.0	N/A	https://monica.im/ https://github.com/soursec/CVEs/tree/main/CVE-2024-48140
https://nvd.nist.gov/vuln/detail/CVE-2024-48139	7.5	Blackbox AI	Command Injection	v1.3.95	N/A	https://www.blackbox.ai/ https://github.com/soursec/CVEs/tree/main/CVE-2024-48139
https://nvd.nist.gov/vuln/detail/CVE-2024-7985	7.5	FileOrganizer – Manage WordPress and Website Files plugin	Unrestricted Upload of File	all versions up to, and including, 1.0.9	N/A	https://wordpress.org/plugins/fileorganizer/ https://www.wordfence.com/threat-intel/vulnerabilities/id/f79164c2-be3b-496d-b747-3e4b60b7fc2b?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-9162	7.2	WP Migration and Backup plugin for WordPress	Code Injection	all versions up to, and including, 7.86	N/A	https://wordpress.org/plugins/all-in-one-wp-migration/ https://www.wordfence.com/threat-intel/vulnerabilities/id/d97c3379-56c9-4261-9a70-3119ec121a40?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2024-10429	7.2	WAVLINK devices	Command Injection	WN530H4, WN530HG4 and WN572HG3 up to 20221028	N/A	https://www.wavlink.com/en_us/index.html https://docs.google.com/document/d/1ktuys5jr7MKwz503QBbEfxZ5mZbXlbvl/
https://nvd.nist.gov/vuln/detail/CVE-2024-50448	7.1	YITH YITH WooCommerce Product	Cross-site Scripting	from n/a through 4.14.1	N/A	https://wordpress.org/plugins/yith-woocommerce-product-add-ons/ https://patchstack.com/database/vulnerability/yith-woocommerce-product-add-ons/wordpress-yith-woocommerce-product-add-ons-plugin-4-14-1-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve

2 CISA/CERT-EU Alerts & Advisories

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	**Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες**	**URL**
CISA Releases Industrial Control Systems Advisories	ICSA-24-298-01 VIMESA VHF/FM Transmitter Blue Plus ICSA-24-298-02 iniNet Solutions SpiderControl SCADA PC HMI Editor ICSA-24-298-03 Deep Sea Electronics DSE855 ICSA-24-268-06 OMNTEC Proteus Tank Monitoring (Update A) ICSA-24-303-01 Siemens InterMesh Subscriber Devices ICSA-24-303-02 Solar-Log Base 15 ICSA-24-303-03 Delta Electronics InfraSuite Device Master	https://www.cisa.gov/news-events/alerts/2024/10/24/cisa-releases-four-industrial-control-systems-advisories https://www.cisa.gov/news-events/alerts/2024/10/29/cisa-releases-three-industrial-control-systems-advisories
Cisco Releases Security Bundle for Cisco ASA, FMC, and FTD Software	Cisco Event Response: October 2024 Cisco ASA, FMC, and FTD Software Security Advisory Bundled Publication	https://www.cisa.gov/news-events/alerts/2024/10/24/cisco-releases-security-bundle-cisco-asa-fmc-and-ftd-software
CISA Adds Known Exploited Vulnerabilities to Catalog	CVE-2024-20481 Cisco ASA and FTD Denial-of-Service Vulnerability CVE-2024-37383 RoundCube Webmail Cross-Site Scripting (XSS) Vulnerability	https://www.cisa.gov/news-events/alerts/2024/10/24/cisa-adds-two-known-exploited-vulnerabilities-catalog
Apple Releases Security Updates for Multiple Products	iOS 18.1 and iPadOS 18.1 iOS 17.7.1 and iPadOS 17.7.1 macOS Sequoia 15.1 macOS Sonoma 14.7.1 macOS Ventura 13.7.1 Safari 18.1 watchOS 11.1 tvOS 18.1 visionOS 2.1	https://www.cisa.gov/news-events/alerts/2024/10/29/apple-releases-security-updates-multiple-products

3 News

News	
Σύντομη περιγραφή / Τίτλος	**URL**
France’s second-largest telecoms provider Free suffered a cyber attack	https://securityaffairs.com/170333/data-breach/free-suffered-a-cyber-attack.html
Mozilla: ChatGPT Can Be Manipulated Using Hex Code	https://www.darkreading.com/application-security/chatgpt-manipulated-hex-code
Windows 11 24H2: The hardware and software blocking the new update	https://www.bleepingcomputer.com/news/microsoft/windows-11-24h2-the-hardware-and-software-blocking-the-new-update/
New Cisco ASA and FTD features block VPN brute-force password attacks	https://www.bleepingcomputer.com/news/security/new-cisco-asa-and-ftd-features-block-vpn-brute-force-password-attacks/
Five Eyes Agencies Launch Startup Security Initiative	https://www.infosecurity-magazine.com/news/five-eyes-agencies-startup/
U.S. Government Issues New TLP Guidance for Cross-Sector Threat Intelligence Sharing	https://thehackernews.com/2024/10/us-government-issues-new-tlp-guidance.html
Delta Launches $500M Lawsuit Against CrowdStrike	https://www.darkreading.com/cyberattacks-data-breaches/delta-launches-500m-lawsuit-crowdstrike

3.1 Breaches

News - Breaches	
Σύντομη περιγραφή / Τίτλος	**URL**
US says Chinese hackers breached multiple telecom providers	https://www.bleepingcomputer.com/news/security/us-says-chinese-hackers-breached-multiple-telecom-providers/
A crime ring compromised Italian state databases reselling stolen info	https://securityaffairs.com/170328/data-breach/a-crime-ring-compromised-italian-state-databases.html
Week in review: Fortinet patches critical FortiManager 0-day, VMware fixes vCenter Server RCE	https://www.helpnetsecurity.com/2024/10/27/week-in-review-fortinet-patches-critical-fortimanager-0-day-vmware-fixes-vcenter-server-rce/

3.2 Vulnerabilities and flaws

News – Vulnerabilities and Flaws	
Σύντομη περιγραφή / Τίτλος	**URL**
Critical Chrome Security Update: Patch for Out-of-Bounds & WebRTC Vulnerability	**https://cybersecuritynews.com/chrome-security-out-of-bounds-webrtc/**
New Attack Lets Hackers Downgrade Windows to Exploit Patched Flaws	https://hackread.com/hackers-downgrade-windows-exploit-patched-flaws/

New Research Reveals Spectre Vulnerability Persists in Latest AMD and Intel Processors	https://thehackernews.com/2024/10/new-research-reveals-spectre.html
Fog Ransomware Exploits SonicWall VPN Vulnerability to Breach Corporate Networks	https://dailysecurityreview.com/security-spotlight/fog-ransomware-exploits-sonicwall-vpn-vulnerability-to-breach-corporate-networks/
Lazarus Group Exploits Google Chrome Vulnerability to Control Infected Devices	https://thehackernews.com/2024/10/lazarus-group-exploits-google-chrome.html

3.3 Potential threats / Threat intelligence

News – Potential Threats / Threat Intelligence	
Σύντομη περιγραφή / Τίτλος	**URL**
New Type of Job Scam Targets Financially Vulnerable Populations	https://www.infosecurity-magazine.com/news/job-scam-targets-financially/
Chinese Hackers Use CloudScout Toolset to Steal Session Cookies from Cloud Services	https://thehackernews.com/2024/10/chinese-hackers-use-cloudscout-toolset.html
Black Basta operators phish employees via Microsoft Teams	https://www.helpnetsecurity.com/2024/10/28/black-basta-operators-phish-employees-via-microsoft-teams/
Russian Malware Campaign Targets Ukrainian Recruits Via Telegram	https://www.infosecurity-magazine.com/news/russian-malware-ukrainian-recruits/
TeamTNT Exploits 16 Million IPs in Malware Attack on Docker Clusters	https://hackread.com/teamtnt-exploits-ips-malware-attack-docker-clusters/
Threat Actors Push ClickFix Fake Browser Updates Using Stolen Credentials	https://www.infostealers.com/article/threat-actors-push-clickfix-fake-browser-updates-using-stolen-credentials/
Russia-linked espionage group UNC5812 targets Ukraine's military with malware	https://securityaffairs.com/170346/cyber-warfare-2/unc5812-targets-ukraines-military-malware.html
China's 'Evasive Panda' APT Debuts High-End Cloud Hijacking	https://www.darkreading.com/cloud-security/china-evasive-panda-apt-cloud-hijacking
Midnight Blizzard conducts large-scale spear-phishing campaign using RDP files	https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/
Massive PSAUX ransomware attack targets 22,000 CyberPanel instances	https://www.bleepingcomputer.com/news/security/massive-psaux-ransomware-attack-targets-22-000-cyberpanel-instances/

3.4 Guides / Tools

News – Guides / Tools	
Σύντομη περιγραφή / Τίτλος	**URL**

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.