Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 12/11/2024 - 14/11/2024

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-2024-10575 https://nvd.nist.gov/vuln/detail/CVE-2024-8938 https://nvd.nist.gov/vuln/detail/CVE-2024-8935	**10**	Schneider Electric products	Missing Authorization	N/A	N/A	https://www.se.com/ww/en/ https://download.schneider-electric.com/doc/SEVD-2024-317-04/SEVD-2024-317-04.pdf https://download.schneider-electric.com/doc/SEVD-2024-317-03/SEVD-2024-317-03.pdf https://download.schneider-electric.com/doc/SEVD-2024-317-02/SEVD-2024-317-02.pdf
https://nvd.nist.gov/vuln/detail/CVE-2024-44102	**10**	Siemens (TeleControl Server Basic 1000 to 5000)	Deserialization of Untrusted Data	Multiple products	N/A	https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10087338 https://cert-portal.siemens.com/productcert/html/ssa-454789.html
https://nvd.nist.gov/vuln/detail/CVE-2024-46888	**9.9**	Siemens (SINEC INS)	Path Traversal	All versions < V1.0 SP2 Update 3	N/A	https://www.siemens.com/us/en/products/automation/industrial-communication/sinec-networkmanagement/sinec-ins-infrastructure-network-services.html https://cert-portal.siemens.com/productcert/html/ssa-915275.html
https://nvd.nist.gov/vuln/detail/CVE-2024-50330	**9.8**	Ivanti Endpoint Manager	SQL Injection	before 2024 November Security Update or 2022 SU6 November Security Update	N/A	https://www.ivanti.com/products/endpoint-manager https://forums.ivanti.com/s/article/Security-Advisory-EPM-November-2024-for-EPM-2024-and-EPM-2022
https://nvd.nist.gov/vuln/detail/CVE-2024-49369	**9.8**	Icinga monitoring system	Improper Certificate Validation	versions starting from 2.4.0	v2.14.3, v2.13.10, v2.12.11, and v2.11.12	https://icinga.com/ https://icinga.com/blog/2024/11/12/critical-icinga-2-security-releases-2-14-3
https://nvd.nist.gov/vuln/detail/CVE-2024-24117	**9.8**	Ruijie RG-NBS2009G-P	Insecure Permissions	v.10.4(1)P2 Release (9736)	N/A	https://www.ruijienetworks.com/ https://github.com/zty-1995/RG-NBS2009G-P-switch/tree/main/Any%20user%20login%20exists
https://nvd.nist.gov/vuln/detail/CVE-2024-39712	**9.1**	Ivanti Connect Secure Ivanti Policy Secure	Argument injection	before version 22.7R2.1 and 9.1R18.7 before version 22.7R1.1	N/A	https://www.ivanti.com/products/connect-secure-vpn https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-ICS-Ivanti-Policy-Secure-IPS-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs
https://nvd.nist.gov/vuln/detail/CVE-2024-10943	**9.1**	Rockwell Automation products	Insecure Storage of	N/A	N/A	https://www.rockwellautomation.com/en-us.html https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1710.html

			Sensitive Information			
https://nvd.nist.gov/vuln/detail/CVE-2024-9465	9.1	Palo Alto Networks Expedition	SQL injection	N/A	N/A	https://www.paloaltonetworks.com/ https://security.paloaltonetworks.com/PAN-SA-2024-0010
https://nvd.nist.gov/vuln/detail/CVE-2024-11113	8.8	Google Chrome	Use After Free	prior to 131.0.6778.69	N/A	https://www.google.com/chrome/ https://chromereleases.googleblog.com/2024/11/stable-channel-update-for-desktop_12.html
https://nvd.nist.gov/vuln/detail/CVE-2024-2208	8.8	HP PC Product (Sound Research SECOMN64 driver)	Uncontrolled Search Path Element	N/A	N/A	https://www.hp.com/us-en/shop/cat/desktops https://support.hp.com/us-en/document/ish_11567250-11567490-16/hpsbhf03987
https://nvd.nist.gov/vuln/detail/CVE-2024-21976	8.8	AMD NPU driver	Improper Input Validation	N/A	N/A	https://www.amd.com/en.html https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7017.html
https://nvd.nist.gov/vuln/detail/CVE-2024-36242	8.8	Intel(R) Processors	Protection Mechanism Failure	N/A	N/A	https://www.intel.com/content/www/us/en/products/details/processors/core.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01196.html
https://nvd.nist.gov/vuln/detail/CVE-2024-23918	8.8	Intel(R) Xeon(R) processor	Improper Sanitization of Custom Special Characters	N/A	N/A	https://www.intel.com/content/www/us/en/products/details/processors/xeon.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01079.html
https://nvd.nist.gov/vuln/detail/CVE-2024-50386	8.5	Apache CloudStack	Improper Input Validation	4.0.0 through 4.18.2.4 and 4.19.0.0 through 4.19.1.2	4.18.2.5 or 4.19.1.3, or later	https://cloudstack.apache.org/ https://cloudstack.apache.org/blog/security-release-advisory-4.18.2.5-4.19.1.3
https://nvd.nist.gov/vuln/detail/CVE-2024-47808	8.4	Siemens (SINEC NMS)	Incorrect Permission Assignment for Critical Resource	All versions < V3.0 SP1	N/A	https://www.siemens.com/global/en/products/automation/industrial-communication/sinec-network-software/networkmanagement.html https://cert-portal.siemens.com/productcert/html/ssa-331112.html
https://nvd.nist.gov/vuln/detail/CVE-2024-38665	8.4	Intel(R) Graphics Drivers	Out-of-bounds Write	N/A	N/A	https://www.intel.com/content/www/us/en/download-center/home.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01132.html
https://nvd.nist.gov/vuln/detail/CVE-2024-36513	8.2	FortiClient Windows version	Privilege Context Switching Error	7.2.4 and below, version 7.0.12 and below, 6.4 all versions	N/A	https://www.fortinet.com/support/product-downloads https://fortiguard.fortinet.com/psirt/FG-IR-24-144
https://nvd.nist.gov/vuln/detail/CVE-2024-36482	8.2	Intel(R) CIP software	Improper Input Validation	before version 2.4.10852	N/A	https://www.intel.com/content/www/us/en/support/topics/idsa-cip.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01182.html
https://nvd.nist.gov/vuln/detail/CVE-2024-36282	8.2	Intel(R) Server Board S2600ST	Improper Input Validation	S2600ST Family BIOS and Firmware Update software all versions	N/A	https://www.intel.com/content/www/us/en/products/details/servers/server-boards/server-board-s2600st.html

						https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01183.html
https://nvd.nist.gov/vuln/detail/CVE-2024-32483	8.2	Intel(R) EMA	Improper Access Control	before version 1.13.1.0	N/A	https://www.intel.com/content/www/us/en/download/19805/intel-endpoint-management-assistant-configuration-tool-intel-ema-configuration-tool.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01201.html
https://nvd.nist.gov/vuln/detail/CVE-2024-10828	8.1	Advanced Order Export For WooCommerce plugin for WordPress	Deserialization of Untrusted Data	all versions up to, and including, 3.5.5	N/A	https://wordpress.org/plugins/woo-order-export-lite/ https://www.wordfence.com/threat-intel/vulnerabilities/id/a1c6eed6-7b3f-4b37-85f8-6613527daa54?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-45827	8	Mesh Wi-Fi router RP562B	OS Command Injection	firmware version v1.0.2 and earlier	N/A	https://neroteam.com/blog/softbank-wi-fi-mesh-rp562b?/softbank-wi-fi-mesh-rp562b https://jvn.jp/en/vu/JVNVU90676195/
https://nvd.nist.gov/vuln/detail/CVE-2024-39368	8	Intel(R) Neural Compressor	SQL Injection	before version v3.0	N/A	https://www.intel.com/content/www/us/en/developer/tools/oneapi/neural-compressor.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01219.html
https://nvd.nist.gov/vuln/detail/CVE-2024-37398	7.8	Ivanti Secure Access Client	Insufficient validation	before 22.7R4	N/A	https://www.ivanti.com/products/secure-unified-client https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-ICS-Ivanti-Policy-Secure-IPS-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs
https://nvd.nist.gov/vuln/detail/CVE-2024-47941	7.8	Siemens (Solid Edge SE2024)	Out-of-bounds Read	All versions < V224.0 Update 9	N/A	https://blogs.sw.siemens.com/solidedge/introducing-solid-edge-2024/ https://cert-portal.siemens.com/productcert/html/ssa-351178.html
https://nvd.nist.gov/vuln/detail/CVE-2024-47783	7.8	Siemens (SIPORT)	Incorrect Permission Assignment for Critical Resource	All versions < V3.4.0	N/A	https://www.siemens.com/global/en/products/buildings/security/access-control/siport.html https://cert-portal.siemens.com/productcert/html/ssa-064257.html
https://nvd.nist.gov/vuln/detail/CVE-2024-29119	7.8	Siemens (Spectrum Power 7)	Incorrect Privilege Assignment	All versions < V24Q3	N/A	https://xcelerator.siemens.com/global/en/all-offerings/products/s/spectrum-power-7-ros.html https://cert-portal.siemens.com/productcert/html/ssa-616032.html
https://nvd.nist.gov/vuln/detail/CVE-2024-47574	7.8	Fortinet FortiClientWindows	Authentication Bypass	version 7.4.0, versions 7.2.4 through 7.2.0, versions 7.0.12 through 7.0.0, and 6.4.10 through 6.4.0	N/A	https://www.fortinet.com/support/product-downloads https://fortiguard.fortinet.com/psirt/FG-IR-24-199
https://nvd.nist.gov/vuln/detail/CVE-2024-40592	7.5	FortiClient MacOS version	Improper Verification	version 7.4.0, version 7.2.4 and below, version 7.0.10 and below, version 6.4.10 and below	N/A	https://docs.fortinet.com/document/forticlient/7.4.1/administration-guide/903183/macos https://fortiguard.fortinet.com/psirt/FG-IR-24-022
https://nvd.nist.gov/vuln/detail/CVE-2024-23666	7.5	Fortinet FortiAnalyzer-BigData	Client-Side Enforcement of Server-Side Security	Multiple versions	N/A	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer-bd.pdf https://fortiguard.fortinet.com/psirt/FG-IR-23-396

https://nvd.nist.gov/vuln/detail/CVE-2023-50176	7.5	Fortinet FortiOS	Session Fixation	version 7.4.0 through 7.4.3 and 7.2.0 through 7.2.7 and 7.0.0 through 7.0.13	N/A	https://docs.fortinet.com/product/fortigate/7.6 https://fortiguard.fortinet.com/psirt/FG-IR-23-475
https://nvd.nist.gov/vuln/detail/CVE-2024-50310	7.5	Siemens (SIMATIC CP 1543-1)	Incorrect Authorization	V4.0 (6GK7543-1AX10-0XE0) (All versions >= V4.0.44 < V4.0.50)	N/A	https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10176733 https://cert-portal.siemens.com/productcert/html/ssa-654798.html
https://nvd.nist.gov/vuln/detail/CVE-2024-41167	7.5	Intel(R) Server Board	Improper Input Validation	M10JNP2SB Family	N/A	https://www.intel.com/content/www/us/en/products/sku/197377/intel-server-board-m10jnp2sb/specifications.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01175.html
https://nvd.nist.gov/vuln/detail/CVE-2024-39609	7.5	Intel(R) Server Board	Improper Access Control	M70KLP	N/A	https://www.intel.com/content/www/us/en/products/details/servers/server-systems/server-system-m70klp.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01175.html
https://nvd.nist.gov/vuln/detail/CVE-2024-31158	7.5	Intel(R) Server Board S2600BP	Improper Input Validation	S2600BP Family	N/A	https://ark.intel.com/content/www/us/en/ark/products/93497/intel-server-board-s2600bpb.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01175.html
https://nvd.nist.gov/vuln/detail/CVE-2024-48989	7.5	PROFINET stack implementation of the IndraDrive	Uncontrolled Resource Consumption	all versions	N/A	https://www.profibus.com/ https://psirt.bosch.com/security-advisories/BOSCH-SA-315415.html
https://nvd.nist.gov/vuln/detail/CVE-2024-4741	7.5	OpenSSL	Use After Free	N/A	FIPS modules in 3.3, 3.2, 3.1 and 3.0	https://www.openssl.org/ https://openssl-library.org/news/secadv/20240528.txt
https://nvd.nist.gov/vuln/detail/CVE-2024-10174	7.3	WP Project Manager – Task, team, and project management plugin	Authorization Bypass	all versions up to, and including, 2.6.13	N/A	https://wordpress.org/plugins/wedevs-project-manager/ https://www.wordfence.com/threat-intel/vulnerabilities/id/dea2d045-d3b4-4b55-8b4f-5baa82a18834?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-21958	7.3	AMD Provisioning Console	Incorrect Default Permissions	N/A	N/A	https://www.amd.com/en/support/downloads/manageability-tools.html https://www.amd.com/en/resources/product-security/bulletin/amd-sb-9007.html
https://nvd.nist.gov/vuln/detail/CVE-2023-32736	7.3	Siemens (SIMATIC S7-PLCSIM V16)	Deserialization of Untrusted Data	Multiple products and versions	N/A	https://support.industry.siemens.com/cs/document/109775861/updates-for-step-7-v16-s7-plcsim-v16-and-wincc-v16?dti=0&lc=en-GR https://cert-portal.siemens.com/productcert/html/ssa-871035.html
https://nvd.nist.gov/vuln/detail/CVE-2024-36488	7.3	Intel(R) DSA	Improper Access Control	before version 24.3.26.8	N/A	https://www.intel.com/content/www/us/en/support/detect.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01200.html
https://nvd.nist.gov/vuln/detail/CVE-2024-49042	7.2	Azure Database for PostgreSQL	Command Injection	N/A	N/A	https://azure.microsoft.com/en-us/products/postgresql https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49042

https://nvd.nist.gov/vuln/detail/CVE-2024-42442	**7.2**	APTIOV (bios/uefi solutions with Aptio)	Improper Restriction of Operations	N/A	N/A	https://www.ami.com/aptio/ https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/2024/AMI-SA-2024004.pdf
https://nvd.nist.gov/vuln/detail/CVE-2024-50572	**7.2**	Siemens (RUGGEDCOM)	Improper Neutralization of Special Elements	Multiple products	N/A	https://www.siemens.com/global/en/products/automation/industrial-communication/ruggedcom.html https://cert-portal.siemens.com/productcert/html/ssa-354112.html

2 CISA/CERT-EU Alerts & Advisories

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	**Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες**	**URL**
Fortinet Releases Security Updates for Multiple Products	FG-IR-23-396 ReadOnly Users Could Run Some Sensitive Operations FG-IR-23-475 FortiOS - SSLVPN Session Hijacking Using SAML Authentication FG-IR-24-144 Privilege Escalation via Lua Auto Patch Function FG-IR-24-199 Named Pipes Improper Access Control	https://www.cisa.gov/news-events/alerts/2024/11/12/fortinet-releases-security-updates-multiple-products
Microsoft Releases November 2024 Security Updates	Microsoft Security Update Guide for November	https://www.cisa.gov/news-events/alerts/2024/11/12/microsoft-releases-november-2024-security-updates
Adobe Releases Security Updates for Multiple Products	Security update available for Adobe Bridge | APSB24-77 Security update available for Adobe Audition | APSB24-83 Security update available for Adobe After Effects | APSB24-85 Security update available for Adobe Substance 3D Painter | APSB24-86 Security update available for Adobe Illustrator| APSB24-87 Security update available for Adobe InDesign | APSB24-88 Security update available for Adobe Photoshop | APSB24-89 Security update available for Adobe Commerce | APSB24-90	https://www.cisa.gov/news-events/alerts/2024/11/12/adobe-releases-security-updates-multiple-products
Ivanti Releases Security Updates for Multiple Products	Ivanti Security Advisory EPM Ivanti Security Advisory Avalanche Ivanti Security Advisory Connect Secure, Ivanti Policy Secure, and Ivanti Security Access Client	https://www.cisa.gov/news-events/alerts/2024/11/12/ivanti-releases-security-updates-multiple-products
Citrix Releases Security Updates for NetScaler and Citrix Session Recording	NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2024-8534 and CVE-2024-8535 Citrix Session Recording Security Bulletin for CVE-2024-8068 and CVE-2024-8069	https://www.cisa.gov/news-events/alerts/2024/11/12/citrix-releases-security-updates-netscaler-and-citrix-session-recording
CISA Adds Known Exploited Vulnerabilities to Catalog	CVE-2021-26086 Atlassian Jira Server and Data Center Path Traversal Vulnerability CVE-2014-2120 Cisco Adaptive Security Appliance (ASA) Cross-Site Scripting (XSS) Vulnerability CVE-2021-41277 Metabase GeoJSON API Local File Inclusion Vulnerability CVE-2024-43451 Microsoft Windows NTLMv2 Hash Disclosure Spoofing Vulnerability CVE-2024-49039 Microsoft Windows Task Scheduler Privilege Escalation Vulnerability	https://www.cisa.gov/news-events/cybersecurity-advisories#definitions

Palo Alto Networks Emphasizes Hardening Guidance	PAN-SA-2024-0015 Important Informational Bulletin: Ensure Access to Management Interface is Secured Tips & Tricks: How to Secure the Management Access of Your Palo Alto Networks Device	https://www.cisa.gov/news-events/alerts/2024/11/13/palo-alto-networks-emphasizes-hardening-guidance

3 News

News	
Σύντομη περιγραφή / Τίτλος	**URL**
DDoS attack targets Israeli credit card readers	https://www.scworld.com/brief/ddos-attack-targets-israeli-credit-card-readers
Halliburton Ransomware Attack Costs Energy Giant $35 Million	https://dailysecurityreview.com/security-spotlight/halliburton-ransomware-attack-costs-energy-giant-35-million/
How a Windows zero-day was exploited in the wild for months (CVE-2024-43451)	https://www.helpnetsecurity.com/2024/11/14/cve-2024-43451-exploited/
OpenText Cybersecurity Unveils 2024's Nastiest Malware	https://www.darkreading.com/cyberattacks-data-breaches/opentext-cybersecurity-unveils-2024-s-nastiest-malware
China’s Volt Typhoon botnet has re-emerged	https://securityaffairs.com/170872/apt/volt-typhoon-botnet-has-re-emerged.html
Critical bug in EoL D-Link NAS devices now exploited in attacks	https://www.bleepingcomputer.com/news/security/critical-bug-in-eol-d-link-nas-devices-now-exploited-in-attacks/
NIS2 Directive: Everything EU Member States and Organizations Need to Know to Prepare and Comply	https://www.infosecurity-magazine.com/blogs/nis2-everything-eu-orgs-need-to/
US govt officials’ communications compromised in recent telecom hack	https://www.bleepingcomputer.com/news/security/chinese-hackers-compromised-us-government-officials-private-communications-in-recent-telecom-breach/

3.1 Breaches

News - Breaches	
Σύντομη περιγραφή / Τίτλος	**URL**
Over 300K Presbyterian Healthcare patients hit by third-party breach	https://www.scworld.com/brief/over-300k-presbyterian-healthcare-patients-hit-by-third-party-breach
Millions of records from MOVEit hack released on dark web	https://www.scworld.com/news/millions-of-records-from-moveit-hack-released-on-dark-web
SelectBlinds Data Breach: 200,000 Customers Impacted by E-Skimming Attack	https://dailysecurityreview.com/security-spotlight/selectblinds-data-breach-200000-customers-impacted-by-e-skimming-attack/
Leaked info of 122 million linked to B2B data aggregator breach	https://www.bleepingcomputer.com/news/security/leaked-info-of-122-million-linked-to-b2b-data-aggregator-breach/

3.2 Vulnerabilities and flaws

News – Vulnerabilities and Flaws	
Σύντομη περιγραφή / Τίτλος	**URL**
Citrix 'Recording Manager' Zero-Day Bug Allows Unauthenticated RCE	https://www.darkreading.com/cloud-security/citrix-recording-manager-zero-day-bug-unauthenticated-rce
OvrC Platform Vulnerabilities Expose IoT Devices to Remote Attacks and Code Execution	https://thehackernews.com/2024/11/ovrc-platform-vulnerabilities-expose.html

3.3 Potential threats / Threat intelligence

News – Potential Threats / Threat Intelligence	
Σύντομη περιγραφή / Τίτλος	**URL**
North Korean hackers create Flutter apps to bypass macOS security	https://www.bleepingcomputer.com/news/security/north-korean-hackers-create-flutter-apps-to-bypass-macos-security/
Aerospace employees targeted with malicious “dream job” offers	https://www.helpnetsecurity.com/2024/11/13/malicious-job-offers-aerospace/
New RustyAttr Malware Targets macOS Through Extended Attribute Abuse	https://thehackernews.com/2024/11/new-rustyattr-malware-targets-macos.html
Asian Threat Actors Use New Techniques to Attack Familiar Targets	https://www.darkreading.com/cyberattacks-data-breaches/asian-threat-actors-use-new-techniques-to-attack-familiar-targets
Russian Hackers Exploit New NTLM Flaw to Deploy RAT Malware via Phishing Emails	https://thehackernews.com/2024/11/russian-hackers-exploit-new-ntlm-flaw.html
Iranian Cybercriminals Target Aerospace Workers via LinkedIn	https://www.darkreading.com/cyberattacks-data-breaches/iranian-cybercriminals-aerospace-workers-linkedin
China-linked hackers stole surveillance data from telecom companies, US says	https://www.reuters.com/technology/cybersecurity/china-affiliated-actors-compromised-networks-multiple-telecom-companies-us-says-2024-11-13/
The China-affiliated group is using the highly modular DeepData framework to target organizations in South Asia.	https://www.darkreading.com/cyberattacks-data-breaches/toolkit-expands-apt41s-surveillance-powers

3.4 Guides / Tools

News – Guides / Tools	
Σύντομη περιγραφή / Τίτλος	**URL**
New ShrinkLocker ransomware decryptor recovers BitLocker password	https://www.bleepingcomputer.com/news/security/new-shrinklocker-ransomware-decryptor-recovers-bitlocker-password/

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.