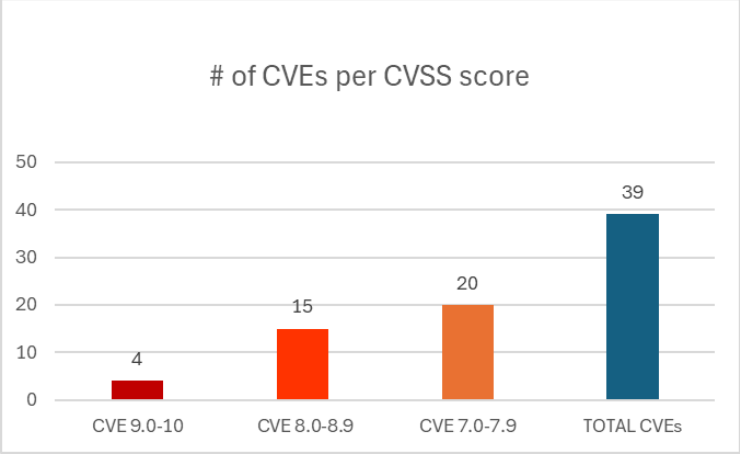
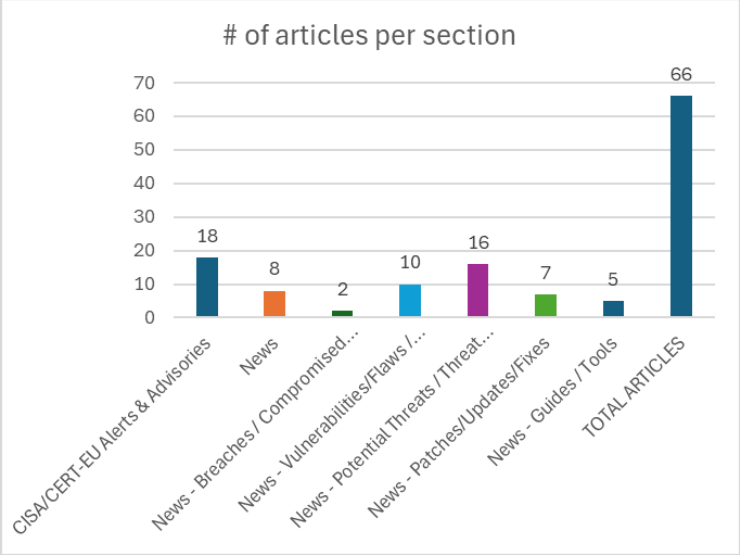
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 10/06/2025 - 13/06/2025





Contents

Common Vulnerabilities and Exposures (CVEs)

URL ευπάθειας (NIST NVD)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2025-5288	9,8	The REST API | Custom API Generator For Cross Platform And Import Export In WP plugin for WordPress	Missing Authorization	versions 1.0.0 to 2.0.3	https://plugins.trac.wordpress.org/browser/import-export-with-custom-rest-api/tags/2.0.3/backend/methods/wot-rapi-import-functions.php#L123 https://wordpress.org/plugins/import-export-with-custom-rest-api/#developers https://www.wordfence.com/threat-intel/vulnerabilities/id/0e2774fc-f028-436c-a8af-3c17378b9743?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-40585	9,5	Energy Services	Incorrect Default Permissions	All versions with G5DFR	https://cert-portal.siemens.com/productcert/html/ssa-345750.html
https://nvd.nist.gov/vuln/detail/CVE-2025-32711	9,3	Copilot	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Ai command injection in M365 Copilot	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32711
https://nvd.nist.gov/vuln/detail/CVE-2025-47110	9,1	Adobe Commerce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')		https://helpx.adobe.com/security/products/magento/apsb25-50.html
https://nvd.nist.gov/vuln/detail/CVE-2025-33064	8,8	Windows Routing and Remote Access Service (RRAS)	Heap-based Buffer Overflow		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33064
https://nvd.nist.gov/vuln/detail/CVE-2025-33066	8,8	Windows Routing and Remote Access Service (RRAS)	Heap-based Buffer Overflow		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33066
https://nvd.nist.gov/vuln/detail/CVE-2025-33073	8,8	Windows SMB	Improper Access Control		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33073

https://nvd.nist.gov/vuln/detail/CVE-2025-47172	8,8	Microsoft Office SharePoint	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47172
https://nvd.nist.gov/vuln/detail/CVE-2025-5491	8,8	Acer ControlCenter	Improper Privilege Management		https://community.acer.com/en/kb/articles/18243-misconfigured-windows-named-pipe-permissions-in-accsvc-exe-allows-for-remote-code-execution?utm_source=community-search&utm_medium=organic-search&utm_term=Vulnerability https://www.twcert.org.tw/en/cp-139-10181-933ae-2.html https://www.twcert.org.tw/tw/cp-132-10180-36818-1.html
https://nvd.nist.gov/vuln/detail/CVE-2025-46840	8,7	Adobe Experience Manager	Improper Authorization	6.5.22	https://helpx.adobe.com/security/products/experience-manager/apsb25-48.html
https://nvd.nist.gov/vuln/detail/CVE-2025-32717	8,4	Microsoft Office Word	Heap-based Buffer Overflow		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32717
https://nvd.nist.gov/vuln/detail/CVE-2025-33067	8,4	Windows Kernel	Improper Privilege Management		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33067

https://nvd.nist.gov/vuln/detail/CVE-2025-40591	8,3	RUGGEDCOM	Client-Side Enforcement of Server-Side Security	RUGGEDCOM ROX MX5000 (All versions < V2.16.5), RUGGEDCOM ROX MX5000RE (All versions < V2.16.5), RUGGEDCOM ROX RX1400 (All versions < V2.16.5), RUGGEDCOM ROX RX1500 (All versions < V2.16.5), RUGGEDCOM ROX RX1501 (All versions < V2.16.5), RUGGEDCOM ROX RX1510 (All versions < V2.16.5), RUGGEDCOM ROX RX1511 (All versions < V2.16.5), RUGGEDCOM ROX RX1512 (All versions < V2.16.5), RUGGEDCOM ROX RX1524 (All versions < V2.16.5), RUGGEDCOM ROX RX1536 (All versions < V2.16.5), RUGGEDCOM ROX RX5000 (All versions < V2.16.5)	https://cert-portal.siemens.com/productcert/html/ssa-301229.html
https://nvd.nist.gov/vuln/detail/CVE-2025-29828	8,1	Windows Cryptographic Services	Missing Release of Memory after Effective Lifetime		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29828
https://nvd.nist.gov/vuln/detail/CVE-2025-32710	8,1	Windows Remote Desktop Services	Use After Free Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32710

https://nvd.nist.gov/vuln/detail/CVE-2025-33070	8,1	Windows Netlogon	Use of Uninitialized Resource		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33070
https://nvd.nist.gov/vuln/detail/CVE-2025-33071	8,1	Windows KDC Proxy Service (KPSSVC)	Use After Free		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33071
https://nvd.nist.gov/vuln/detail/CVE-2025-41663	8,1	WWH servers	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')		https://certvde.com/en/advisories/VDE-2025-052
https://nvd.nist.gov/vuln/detail/CVE-2025-43586	8,1	Adobe Commerce	Improper Access Control	versions 2.4.8, 2.4.7-p5, 2.4.6-p10, 2.4.5-p12, 2.4.4-p13 and earlier	https://helpx.adobe.com/security/products/magento/apsb25-50.html
https://nvd.nist.gov/vuln/detail/CVE-2025-32712	7,8	Windows Win32K - GRFX	Use After Free		https://nvd.nist.gov/vuln/detail/CVE-2025-32712
https://nvd.nist.gov/vuln/detail/CVE-2025-32713	7,8	Windows Common Log File System Driver	Heap-based Buffer Overflow		https://nvd.nist.gov/vuln/detail/CVE-2025-32713
https://nvd.nist.gov/vuln/detail/CVE-2025-32714	7,8	Windows Installer	Improper Access Control		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32714
https://nvd.nist.gov/vuln/detail/CVE-2025-32716	7,8	Windows Media	Out-of-bounds Read		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32716
https://nvd.nist.gov/vuln/detail/CVE-2025-32718	7,8	Windows SMB	Integer Overflow or Wraparound Heap-based Buffer Overflow		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32718
https://nvd.nist.gov/vuln/detail/CVE-2025-33075	7,8	Windows Installer	Improper Link Resolution Before File Access ('Link Following')		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33075
https://nvd.nist.gov/vuln/detail/CVE-2025-43577	7,8	Acrobat Reader	Use After Free	24.001.30235, 20.005.30763, 25.001.20521 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb25-57.html

https://nvd.nist.gov/vuln/detail/CVE-2025-47955	7,8	Windows Remote Access Connection Manager			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47955
https://nvd.nist.gov/vuln/detail/CVE-2025-47962	7,8	Windows SDK	Improper Access Control		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47962
https://nvd.nist.gov/vuln/detail/CVE-2025-47968	7,8	Microsoft AutoUpdate (MAU)	Improper Input Validation		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47968
https://nvd.nist.gov/vuln/detail/CVE-2025-5335	7,8	Autodesk	Untrusted Search Path		https://www.autodesk.com/trust/security-advisories/adsk-sa-2025-0010
https://nvd.nist.gov/vuln/detail/CVE-2025-25032	7,5	IBM Cognos Analytics	llocation of Resources Without Limits or Throttling	11.2.0, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 12.0.0, 12.0.1, 12.0.2, 12.0.3, and 12.0.4	https://www.ibm.com/support/pages/node/7234674
https://nvd.nist.gov/vuln/detail/CVE-2025-30399	7,5	.NET and Visual Studio	Untrusted Search Path		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-30399
https://nvd.nist.gov/vuln/detail/CVE-2025-32724	7,5	Windows Local Security Authority Subsystem Service (LSASS)	Uncontrolled Resource Consumption		https://nvd.nist.gov/vuln/detail/CVE-2025-32724
https://nvd.nist.gov/vuln/detail/CVE-2025-33050	7,5	Windows DHCP Server	Protection Mechanism Failure		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33050
https://nvd.nist.gov/vuln/detail/CVE-2025-33056	7,5	Microsoft Local Security Authority Server (lsasrv)	Improper Access Control		https://nvd.nist.gov/vuln/detail/CVE-2025-33056
https://nvd.nist.gov/vuln/detail/CVE-2025-33068	7,5	Windows Standards-Based Storage Management Service			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33068

https://nvd.nist.gov/vuln/detail/CVE-2025-5969	7,4	D-Link	Stack-based Buffer Overflow Improper Restriction of Operations within the Bounds of a Memory Buffer	D-Link DIR-632 FW103B08	https://github.com/xiaobor123/vul-finds/tree/main/vul-find-dir632-dlink-FUN_00425fd8 https://github.com/xiaobor123/vul-finds/tree/main/vul-find-dir632-dlink-FUN_00425fd8#poc https://vuldb.com/?ctiid.311845 https://vuldb.com/?id.311845 https://vuldb.com/?submit.592336 https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-32721	7,3	Windows Recovery Driver	Improper Link Resolution Before File Access ('Link Following')		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32721
https://nvd.nist.gov/vuln/detail/CVE-2025-47959	7,1	Visual Studio	Improper Neutralization of Special Elements used in a Command ('Command Injection')		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47959

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Releases Cybersecurity Advisory on SimpleHelp RMM Vulnerability		https://www.cisa.gov/news-events/alerts/2025/06/12/cisa-releases-cybersecurity-advisory-simplehelp-rmm-vulnerability
Ransomware Actors Exploit Unpatched SimpleHelp Remote Monitoring and Management to Compromise Utility Billing Software Provider		https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-163a
CISA Releases Ten Industrial Control Systems Advisories	▪ ICSA-25-162-01 Siemens Tecnomatix Plant Simulation ▪ ICSA-25-162-02 Siemens RUGGEDCOM APE1808 ▪ ICSA-25-162-03 Siemens SCALANCE and RUGGEDCOM ▪ ICSA-25-162-04 Siemens SCALANCE and RUGGEDCOM ▪ ICSA-25-162-05 Siemens SIMATIC S7-1500 CPU Family ▪ ICSA-25-162-06 Siemens Energy Services ▪ ICSA-25-162-07 AVEVA PI Data Archive ▪ ICSA-25-162-08 AVEVA PI Web API ▪ ICSA-25-162-09 AVEVA PI Connector for CygNet ▪ ICSA-25-162-10 PTZOptics and Other Pan-Tilt-Zoom Cameras	https://www.cisa.gov/news-events/alerts/2025/06/12/cisa-releases-ten-industrial-control-systems-advisories

PTZOptics and Other Pan-Tilt-Zoom Cameras		https://www.cisa.gov/news-events/ics-advisories/icsa-25-162-10
AVEVA PI Connector for CygNet		https://www.cisa.gov/news-events/ics-advisories/icsa-25-162-09
AVEVA PI Web API		https://www.cisa.gov/news-events/ics-advisories/icsa-25-162-08
AVEVA PI Data Archive		https://www.cisa.gov/news-events/ics-advisories/icsa-25-162-07
Siemens Energy Services		https://www.cisa.gov/news-events/ics-advisories/icsa-25-162-06
Siemens SIMATIC S7-1500 CPU Family		https://www.cisa.gov/news-events/ics-advisories/icsa-25-162-05
Siemens SCALANCE and RUGGEDCOM		https://www.cisa.gov/news-events/ics-advisories/icsa-25-162-04
Siemens SCALANCE and RUGGEDCOM		https://www.cisa.gov/news-events/ics-advisories/icsa-25-162-03
Siemens RUGGEDCOM APE1808		https://www.cisa.gov/news-events/ics-advisories/icsa-25-162-02
Siemens Tecnomatix Plant Simulation		https://www.cisa.gov/news-events/ics-advisories/icsa-25-162-01
CISA Adds Two Known Exploited Vulnerabilities to Catalog	▪ CVE-2025-24016 Wazuh Server Deserialization of Untrusted Data Vulnerability ▪ CVE-2025-33053 Web Distributed Authoring and Versioning (WebDAV) External Control of File Name or Path Vulnerability	https://www.cisa.gov/news-events/alerts/2025/06/10/cisa-adds-two-known-exploited-vulnerabilities-catalog
CISA Releases Four Industrial Control Systems Advisories	▪ ICSA-25-160-01 SinoTrack GPS Receiver ▪ ICSA-25-160-02 Hitachi Energy Relion 670, 650, SAM600-IO Series ▪ ICSMA-25-160-01 MicroDicom DICOM Viewer ▪ ICSA-25-140-11 Assured Telematics Inc (ATI) Fleet Management System (Update A)	https://www.cisa.gov/news-events/alerts/2025/06/10/cisa-releases-four-industrial-control-systems-advisories

MicroDicom DICOM Viewer		https://www.cisa.gov/news-events/ics-medical-advisories/icsma-25-160-01
Hitachi Energy Relion 670, 650, SAM600-IO Series		https://www.cisa.gov/news-events/ics-advisories/icsa-25-160-02
SinoTrack GPS Receiver		https://www.cisa.gov/news-events/ics-advisories/icsa-25-160-01

News

Σύντομη περιγραφή / Τίτλος	URL
DragonForce Ransomware Group – The Rise of a Relentless Cyber Threat in 2025	https://cybersecuritynews.com/dragonforce-ransomware-group/
Microsoft Outlook's New Two-Click View for Encrypted Emails Protects You From Accidental Exposure	https://cybersecuritynews.com/outlooks-two-click-view-encrypted-emails/
CISA Releases Guide to Protect Network Edge Devices From Hackers	https://cybersecuritynews.com/cisa-guide-network-edge-devices-2/
Hackers Advertising New Blackhat Tool Nytheon AI on Popular Hacking Forums	https://cybersecuritynews.com/nytheon-ai-blackhat-tool/
Top 3 Evasion Techniques In Phishing Attacks: Real Examples Inside	https://cybersecuritynews.com/top-3-evasion-techniques-in-phishing-attacks-real-examples-inside/
Operation Secure: 20,000 Malicious IPs and Domains Linked to 69 Malware Variants Dismantled	https://cybersecuritynews.com/operation-secure/
Microsoft to Block Attachments in Outlook Web & Windows Used by Threat Actors	https://cybersecuritynews.com/microsoft-block-outlook-attachments/
Microsoft Teams New Audit Log Feature Allows Admins to Track Users Actions	https://cybersecuritynews.com/microsoft-teams-audit-log/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Threat Actors Compromise 270+ Legitimate Websites With Malicious JavaScript Using JSFireTruck Obfuscation	https://cybersecuritynews.com/threat-actors-compromise-270-legitimate-websites-with-malicious-javascript/
40,000+ Internet-connected Cameras Exposed Streaming Live on The Internet	https://cybersecuritynews.com/40000-internet-connected-cameras-exposed/

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
PoC Exploit Released for Critical WebDAV 0-Day RCE Vulnerability Exploited by APT Hackers	https://cybersecuritynews.com/webdav-0-day-rce-vulnerability-poc/
Palo Alto Networks PAN-OS Vulnerability Enables Admin to Execute Root User Actions	https://cybersecuritynews.com/pan-os-web-interface-vulnerability/
CyberEYE RAT Disables Windows Defender Using PowerShell and Registry Manipulations	https://cybersecuritynews.com/cybereye-rat-disable-windows-defender-using-powershell/
Trend Micro Apex One Vulnerability Allow Attackers to Inject Malicious Code	https://cybersecuritynews.com/trend-micro-apex-one-vulnerability/
Windows SMB Client Zero-Day Vulnerability Exploited Using Reflective Kerberos Relay Attack	https://cybersecuritynews.com/windows-smb-client-zero-day-vulnerability/
0-Click Microsoft 365 Copilot Vulnerability Let Attackers Exfiltrates Sensitive Data Abusing Teams	https://cybersecuritynews.com/zero-click-microsoft-365-copilot-vulnerability/
Windows Task Scheduler Vulnerability Let Attackers Escalate Privileges	https://cybersecuritynews.com/windows-task-scheduler-vulnerability/
Windows Common Log File System Driver Vulnerability Let Attackers Escalate Privileges	https://cybersecuritynews.com/windows-common-log-file-system-vulnerability/
Microsoft Office Vulnerabilities Let Attackers Execute Remote Code	https://cybersecuritynews.com/microsoft-office-vulnerabilities/
Windows WEBDAV 0-Day RCE Vulnerability Actively Exploited in the Wild – All Versions Affected	https://cybersecuritynews.com/windows-webdav-0-day-actively-exploited/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Microsoft Patched Windows Server 2025 Restart Bug that Disconnects AD Domain Controller	https://cybersecuritynews.com/microsoft-patched-windows-server-2025-restart-bug/
Firefox Patches Multiple Vulnerabilities That Could Lead to Browser Crash	https://cybersecuritynews.com/firefox-patches-multiple-vulnerabilities/
Microsoft Teams New Update Enhances Productivity & Customization	https://cybersecuritynews.com/microsoft-teams-update-productivity/
KB5060999 – Microsoft Releases Windows 11 Cumulative Update for Enhanced Security	https://cybersecuritynews.com/kb5060999-windows-11-cumulative-update/
Windows 11 Cumulative Updates KB5060842 Released with June Patch Tuesday	https://cybersecuritynews.com/windows-11-cumulative-updates-kb5060842-released/
Fortinet Security Update: Critical Patch Addressing Multiple Vulnerabilities Across Products	https://cybersecuritynews.com/fortinet-security-update/
Microsoft Patch Tuesday June 2025 – Exploited zero-day and Other 65 Vulnerabilities Patched	https://cybersecuritynews.com/microsoft-patch-tuesday-june-2025/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Google Vulnerability Let Attackers Access Any Google User's Phone Number	https://cybersecuritynews.com/google-vulnerability-leaks-user-phone-number/
Ivanti Workspace Control Vulnerabilities Let Attackers Decrypt Stored SQL Credentials	https://cybersecuritynews.com/ivanti-workspace-control-vulnerabilities/
Fortinet OS Command Injection Vulnerability Lets Attackers Execute Unauthorised Code on FortiAnalyzer-Cloud	https://cybersecuritynews.com/fortinet-os-command-injection-vulnerability/
Critical SAP NetWeaver Vulnerability Let Attackers Bypass Authorization Checks	https://cybersecuritynews.com/critical-sap-netweaver-vulnerability/
Threat Actors Leverages DeepSeek-R1 Popularity to Attack Users Running Windows Devices	https://cybersecuritynews.com/threat-actors-leverages-deepseek-r1-popularity/
OpenPGP.js Vulnerability Let Attackers Spoof Message Signature Verification	https://cybersecuritynews.com/openpgp-js-vulnerability/
Don't Click 'Unsubscribe' Links Blindly It May Leads to Loss of Credentials	https://cybersecuritynews.com/dont-click-unsubscribe-links-blindly/
AitM Phishing Attacks Targeting Microsoft 365 and Google to Steal Login Credentials	https://cybersecuritynews.com/aitm-phishing-attacks-targeting-microsoft-365/
Threat Actors Allegedly Selling MaaS Botnet on Hackers Forums	https://cybersecuritynews.com/maas-botnet-on-hackers-forums/
New Secure Boot Bypass Vulnerability Let Attackers Install Malware in PCs and Servers Boot Process	https://cybersecuritynews.com/new-secure-boot-bypass-vulnerability/
CoreDNS Vulnerability Let Attackers Exhaust Server Memory Via Amplification Attack	https://cybersecuritynews.com/coredns-vulnerability-exhaust-server-memory/
Microsoft Outlook Vulnerability Let Attackers Execute Arbitrary Code Remotely	https://cybersecuritynews.com/microsoft-outlook-rce-vulnerability/
Multiple Chrome Vulnerabilities Allow Attackers to Execute Malicious Code Remotely	https://cybersecuritynews.com/multiple-chrome-rce-vulnerabilities/
Beware of Instagram Growth That Steals User Login Credentials & Send to Attacker Server	https://cybersecuritynews.com/beware-of-instagram-growth-that-steals-user-login-credentials/
APT Hackers Exploited Windows WebDAV 0-Day RCE Vulnerability in the Wild to Deploy Malware	https://cybersecuritynews.com/windows-webdav-0-day/
FortiOS SSL-VPN Vulnerability Let Attackers Access full SSL-VPN settings	https://cybersecuritynews.com/fortios-ssl-vpn-vulnerability/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Windows Security Best Practices – Protecting Active Directory Environments	https://cybersecuritynews.com/windows-security/
Hardening Linux Servers – A Comprehensive Cybersecurity Checklist	https://cybersecuritynews.com/hardening-linux-servers/
Threat Hunting 101 – Proactive Cybersecurity Strategies for Experts	https://cybersecuritynews.com/threat-hunting-2/
Blockchain Security – Protecting Decentralized Applications	https://cybersecuritynews.com/blockchain-security-2/
Phishing Defense Strategies – Advanced Techniques for Email Security	https://cybersecuritynews.com/phishing-defense-strategies/

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.

Annex – Websites with vendor specific vulnerabilities

Ο πίνακας περιέχει websites από κατασκευαστές που προσφέρουν πληροφορίες σχετικές με ευπάθειες που εμφανίζονται στα προϊόντα τους.

Vendor name / Platform	URL
Wordpress	Wordfence Intelligence Vulnerability Database API https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/ Scan your WordPress website, https://wpscan.com/scan/
Oracle	Critical Patch Updates, Security Alerts and Bulletins, https://www.oracle.com/security-alerts/
Fortinet	Fortinet products, https://www.fortiguard.com/psirt
IBM	Security bulletins, https://cloud.ibm.com/status/security Research, Collaborate and Act on threat intelligence, https://exchange.xforce.ibmcloud.com/
MS Windows	The Microsoft Security Response Center (MSRC), https://msrc.microsoft.com/update-guide/
SAP	SAP Security Notes, https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html
Dell	Security Advisories, Notices and Resources, https://www.dell.com/support/security/en-us
HPE	HPE Security Bulletin Library, https://support.hpe.com/connect/s/securitybulletinlibrary Security Bulletins, https://support.hp.com/us-en/security-bulletins
Cisco	Cisco Security Advisories, https://sec.cloudapps.cisco.com/security/center/publicationListing.x
Palo Alto	Palo Alto Networks Security Advisories, https://security.paloaltonetworks.com/
Ivanti	Security Advisory, https://www.ivanti.com/blog/topics/security-advisory
Mozilla	Mozilla Foundation Security Advisories, https://www.mozilla.org/en-US/security/advisories/
Android	Android Security Bulletins, https://source.android.com/docs/security/bulletin/asb-overview
Zyxel	Security Advisories, https://www.zyxel.com/global/en/support/security-advisories
D-Link	Global Security Advisories, Responses, and Notices, https://supportannouncement.us.dlink.com/
Adobe	Security Bulletins and Advisories, https://helpx.adobe.com/security/security-bulletin.html
Siemens	Siemens ProductCERT and Siemens CERT, https://www.siemens.com/global/en/products/services/cert.html
Splunk	Splunk Security Advisories, https://advisory.splunk.com/