Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 04/02/2025 - 07/02/2025

Contents

1 Common Vulnerabilities and Exposures (CVEs)

URL ευπάθειας (NIST NVD)	CVSSv 3	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-2025-24786	10	WhoDB	Path Traversal	N/A	0.45.0	https://whodb.clidey.com/ https://github.com/clidey/whodb/security/advisories/GHSA-9r4c-jwx3-3j76
https://nvd.nist.gov/vuln/detail/CVE-2025-20124	9.9	Cisco ISE	Deserialization of Untrusted Data	N/A	N/A	https://www.cisco.com/site/us/en/products/security/identity-services-engine/index.html https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multivuls-FTW9AOXF
https://nvd.nist.gov/vuln/detail/CVE-2024-9643	9.8	Four-Faith F3x36 router	Active Debug Code	firmware v2.0.0	N/A	https://www.fourfaith.com/f3x36-fdd-lte-industrial-4g-router.html https://talosintelligence.com/vulnerability_reports/TALOS-2023-1752
https://nvd.nist.gov/vuln/detail/CVE-2025-0890	9.8	Zyxel VMG4325-B10A	Improper Authentication	firmware version 1.00(AAFR.4)C0_20170615	N/A	https://www.zyxelguard.com/VMG4325-B10A.asp?srsltid=AfmBOorRWYXB7U8g-qyynxYxCcVKcrJpY7Jz45g4b_xfBp960CSYTWMN https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025
https://nvd.nist.gov/vuln/detail/CVE-2025-22204	9.8	Joomla	Improper Control of Generation of Code ('Code Injection')	before 11.0.0	N/A	https://www.joomla.org/ https://regularlabs.com/sourcerer
https://nvd.nist.gov/vuln/detail/CVE-2025-1061	9.8	Nextend Social Login Pro plugin for WordPress	Authentication Bypass Using an Alternate Path or Channel	versions up to, and including, 3.1.16	N/A	https://wordpress.org/plugins/nextend-facebook-connect/ https://www.wordfence.com/threat-intel/vulnerabilities/id/6494e54c-db04-41f9-8b91-6ad12528cf01?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-0674	9.8	Elber Communications Equipment	Authentication Bypass Using an Alternate Path or Channel	N/A	N/A	https://github.com/advisories/GHSA-prgf-4jmg-r3v9 https://www.cisa.gov/news-events/ics-advisories/icsa-25-035-03
https://nvd.nist.gov/vuln/detail/CVE-2025-22992	9.8	Emoncms project	SQL Injection	>= 11.6.9	N/A	https://emoncms.org/ https://github.com/emoncms/emoncms/issues/1916

https://nvd.nist.gov/vuln/detail/CVE-2024-51547	9.8	ABB ASPECT-Enterprise	Use of Hard-coded Credentials	ASPECT-Enterprise: through 3.08.03; NEXUS Series: through 3.08.03; MATRIX Series: through 3.08.03	N/A	https://library.e.abb.com/public/b7a2ed1e4f6641c4999cf875324b3b55/DS0112%20ASPECT-Enterprise.pdf https://search.abb.com/library/Download.aspx?DocumentID=9AKK108470A6775&LanguageCode=en&DocumentPartId=pdf%20-%20Public%20Advisory&Action=Launch
https://nvd.nist.gov/vuln/detail/CVE-2025-1066	9.8	OpenPLC_V3	Unrestricted Upload of File with Dangerous Type	N/A	N/A	https://github.com/thiagoralves/OpenPLC_v3 https://medium.com/@alimuhammadsecured/cyberforce-2024-how-i-found-my-first-cve-openplcv3-16c058b114b0
https://nvd.nist.gov/vuln/detail/CVE-2024-57520	9.8	Asterisk	Incorrect Permission Assignment for Critical Resource	v22	N/A	https://www.asterisk.org/community/documentation/ https://gist.github.com/hyp164D1/ae76ab25acfbe263b2ed7b24b6e5c621
https://nvd.nist.gov/vuln/detail/CVE-2025-0665	9.8	libcurl	Multiple Releases of Same Resource or Handle	N/A	N/A	https://curl.se/libcurl/ https://curl.se/docs/CVE-2025-0665.html
https://nvd.nist.gov/vuln/detail/CVE-2025-0960	9.8	AutomationDirect C-more EA9 HMI	Classic Buffer Overflow	N/A	N/A	https://www.automationdirect.com/c-more/home https://community.automationdirect.com/s/cybersecurity/security-advisories https://www.cisa.gov/news-events/ics-advisories/icsa-25-035-08
https://nvd.nist.gov/vuln/detail/CVE-2023-5878	9.1	Honeywell OneWireless Wireless Device Manager	Command Injection	R310.x, R320.x, R321.x, R322.1, R322.2, R323.x, R330.1	R322.3, R330.2	https://process.honeywell.com/us/en/products/wireless/onewireless-network/wireless-device-manager https://process.honeywell.com/
https://nvd.nist.gov/vuln/detail/CVE-2024-51450	9.1	IBM Security Verify Directory	OS Command Injection	10.0.0 through 10.0.3	N/A	https://www.ibm.com/docs/en/svd/10.0.2?topic=overview-security-verify-directory https://www.ibm.com/support/pages/node/7182558
https://nvd.nist.gov/vuln/detail/CVE-2025-23114	9	Veeam Updater	Man-in-the-Middle	N/A	N/A	https://www.veeam.com/products/downloads/latest-version.html https://www.veeam.com/kb4712
https://nvd.nist.gov/vuln/detail/CVE-2024-39272	9	ClearML Enterprise Server	Cross-site Scripting	3.22.5-1533	N/A	https://clear.ml/clearml-enterprise https://www.talosintelligence.com/vulnerability_reports/TALOS-2024-2110
https://nvd.nist.gov/vuln/detail/CVE-2025-23058	8.8	ClearPass Policy Manager	escalation of privileges	N/A	N/A	https://www.hpe.com/asia_pac/en/aruba-clearpass-policy-manager.html https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04784en_us&docLocale=en_US
https://nvd.nist.gov/vuln/detail/CVE-2025-23015	8.8	Apache Cassandra	Privilege Defined With Unsafe Actions	through 3.0.30, 3.11.17, 4.0.15, 4.1.7, 5.0.2	3.0.31, 3.11.18, 4.0.16, 4.1.8, 5.0.3	https://cassandra.apache.org/_/index.html http://www.openwall.com/lists/oss-security/2025/02/03/2 https://lists.apache.org/thread/jmks4msbgkl65ssg69x728sv1m0hwz3s

https://nvd.nist.gov/vuln/detail/CVE-2025-0304	8.8	OpenHarmony	Use After Free	v4.1.2	N/A	https://en.wikipedia.org/wiki/OpenHarmony https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-02.md
https://nvd.nist.gov/vuln/detail/CVE-2025-21408	8.8	Microsoft Edge	Access of Resource Using Incompatible Type ('Type Confusion')	N/A	N/A	https://www.microsoft.com/en-us/edge https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21408
https://nvd.nist.gov/vuln/detail/CVE-2025-23236	8.8	Defense Platform Home Edition	Classic Buffer Overflow	Ver.3.9.51.x and earlier	N/A	https://www.hummingheads.co.jp/english/index.html https://www.hummingheads.co.jp/dep/storelist/
https://nvd.nist.gov/vuln/detail/CVE-2025-24326 https://nvd.nist.gov/vuln/detail/CVE-2025-23239 https://nvd.nist.gov/vuln/detail/CVE-2025-20029	8.8	BIG-IP Advanced WAF/ASM, iControl REST endpoint, BIG-IP TMOS Shell (tmsh)	Out-of-bounds Write Command Injection OS Command Injection	N/A	N/A	https://www.f5.com/products https://my.f5.com/manage/s/article/K000140950 https://my.f5.com/manage/s/article/K000138757 https://my.f5.com/manage/s/article/K000148587
https://nvd.nist.gov/vuln/detail/CVE-2024-37358	8.6	Apache James	Improper Input Validation	N/A	3.7.6 and 3.8.2	https://james.apache.org/ https://lists.apache.org/thread/1pxsh11v5s3fkvhnqvkmlqwt3fgpcrqc
https://nvd.nist.gov/vuln/detail/CVE-2022-31764	8.5	Apache ShardingSphere ElasticJob-UI	Improper Control of Dynamically-Managed Code Resources	N/A	ElasticJob-UI 3.0.2	https://shardingsphere.apache.org/elasticjob/current/en/downloads/ https://lists.apache.org/thread/pg0k223m4hsnnzg4nh7lxvdxxgbkrlqb
https://nvd.nist.gov/vuln/detail/CVE-2024-56135	8.4	Progress LoadMaster	Improper Input Validation	7.2.55.0 to 7.2.60.1 (inclusive) From 7.2.49.0 to 7.2.54.12 (inclusive) 7.2.48.12 and all prior versions ECS All prior versions to 7.2.60.1 (inclusive)	N/A	https://kemptechnologies.com/kemp-load-balancers https://community.progress.com/s/article/LoadMaster-Security-Vulnerability-CVE-2024-56131-CVE-2024-56132-CVE-2024-56133-CVE-2024-56134-CVE-2024-56135
https://nvd.nist.gov/vuln/detail/CVE-2025-25246	8.1	NETGEAR XR1000	Code Injection	before 1.0.0.74, XR1000v2 before 1.1.0.22, and XR500 before 2.3.2.134	N/A	https://www.netgear.com/home/online-gaming/routers/xr1000/ https://kb.netgear.com/000066558/Security-Advisory-for-Unauthenticated-RCE-on-Some-WiFi-Routers-PSV-2023-0039
https://nvd.nist.gov/vuln/detail/CVE-2025-0413	7.8	Parallels Desktop Technical Data Reporter	Improper Link Resolution Before File Access ('Link Following')	N/A	N/A	https://www.parallels.com/ https://kb.parallels.com/130212 https://www.zerodayinitiative.com/advisories/ZDI-25-082/
https://nvd.nist.gov/vuln/detail/CVE-2024-48394	7.8	NDD Print solution	Time-of-check Time-of-use (TOCTOU) Race Condition	5.24.3 and before	N/A	https://ndd.tech/us-en/ndd-print/ https://helpcenter-nddprint.ndd.tech/pt/seguranca-e-compliance/Current/dezembro-2024#0

https://nvd.nist.gov/vuln/detail/CVE-2025-20176	7.7	Cisco IOS Software	improper error handling	SNMP versions 1, 2c, and 3	N/A	https://www.cisco.com/c/en/us/products/ios-nx-os-software/index.html https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-dos-sdxnSUcW
https://nvd.nist.gov/vuln/detail/CVE-2025-24648	7.5	Admin and Site Enhancements (ASE)	Incorrect Privilege Assignment	from n/a through 7.6.2.1	N/A	https://www.wpase.com/ https://patchstack.com/database/wordpress/plugin/admin-site-enhancements/vulnerability/wordpress-admin-and-site-enhancements-ase-plugin-7-6-1-1-privilege-escalation-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-39564	7.5	Juniper Networks Junos	Double Free	Junos OS: * from 22.4 before 22.4R3-S4. Junos OS Evolved: * from 22.4 before 22.4R3-S4-EVO.	N/A	https://www.juniper.net/us/en/products/network-operating-system/junos-os.html https://supportportal.juniper.net/JSA83011
https://nvd.nist.gov/vuln/detail/CVE-2024-2878	7.5	GitLab CE/EE	Allocation of Resources Without Limits or Throttling	starting from 15.7 prior to 16.9.7, starting from 16.10 prior to 16.10.5, and starting from 16.11 prior to 16.11.2	N/A	https://about.gitlab.com/install/ce-or-ee/ https://about.gitlab.com/releases/2024/05/08/patch-release-gitlab-16-11-2-released/
https://nvd.nist.gov/vuln/detail/CVE-2025-0509	7.3	Sparkle	Files or Directories Accessible to External Parties	before version 2.6.4	N/A	https://sparkle-project.org/ https://security.netapp.com/advisory/ntap-20250124-0008/ https://sparkle-project.org/documentation/security-and-reliability/
https://nvd.nist.gov/vuln/detail/CVE-2024-23690	7.2	Netgear FVS336Gv2	OS Command Injection	FVS336Gv2 and FVS336Gv3	N/A	https://www.netgear.com/support/product/fvs336gv2/ https://vulncheck.com/advisories/netgear-fvs336g-rce
https://nvd.nist.gov/vuln/detail/CVE-2024-54171	7.1	IBM EntireX	Improper Restriction of XML External Entity Reference	11.1	N/A	https://community.ibm.com/community/user/ibmz-and-linuxone/blogs/gadi-benedek/2024/09/25/introducing-ibms-entirex-and-applinx https://www.ibm.com/support/pages/node/7182693
https://nvd.nist.gov/vuln/detail/CVE-2024-49352	7.1	IBM Cognos Analytics	Improper Restriction of XML External Entity Reference	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	N/A	https://www.ibm.com/docs/en/cognos-analytics/11.1.0?topic=started-getting-cognos-analytics https://www.ibm.com/support/pages/node/7181480

2 CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Releases Industrial Control Systems Advisories	ICSA-25-035-01 Western Telematic Inc NPS Series, DSM Series, CPM Series ICSA-25-035-02 Rockwell Automation 1756-L8zS3 and 1756-L3zS3 ICSA-25-035-03 Elber Communications Equipment ICSA-25-035-04 Schneider Electric Modicon M580 PLCs, BMENOR2200H and EVLink Pro AC ICSA-25-035-05 Schneider Electric Web Designer for Modicon ICSA-25-035-06 Schneider Electric Modicon M340 and BMXNOE0100/0110, BMXNOR0200H ICSA-25-035-07 Schneider Electric Pro-face GP-Pro EX and Remote HMI ICSA-25-035-08 AutomationDirect C-more EA9 HMI ICSA-23-299-03 Ashlar-Vellum Cobalt, Graphite, Xenon, Argon, Lithium (Update A) ICSA-25-037-01 Schneider Electric EcoStruxure Power Monitoring Expert (PME) ICSA-25-037-02 Schneider Electric EcoStruxure ICSA-25-037-03 ABB Drive Composer ICSA-25-037-04 Trimble Cityworks ICSMA-25-037-01 MicroDicom DICOM Viewer ICSMA-25-037-02 Orthanc Server	https://www.cisa.gov/news-events/alerts/2025/02/04/cisa-releases-nine-industrial-control-systems-advisories https://www.cisa.gov/news-events/alerts/2025/02/06/cisa-releases-six-industrial-control-systems-advisories
CISA Adds Known Exploited Vulnerabilities to Catalog	CVE-2024-45195 Apache OFBiz Forced Browsing Vulnerability CVE-2024-29059 Microsoft .NET Framework Information Disclosure Vulnerability CVE-2018-9276 Paessler PRTG Network Monitor OS Command Injection Vulnerability CVE-2018-19410 Paessler PRTG Network Monitor Local File Inclusion Vulnerability CVE-2025-0411 7-Zip Mark of the Web Bypass Vulnerability	https://www.cisa.gov/news-events/alerts/2025/02/04/cisa-adds-four-known-exploited-vulnerabilities-catalog https://www.cisa.gov/news-events/alerts/2025/02/06/cisa-adds-five-known-exploited-vulnerabilities-catalog https://www.cisa.gov/news-events/alerts/2025/02/05/cisa-adds-one-known-exploited-vulnerability-catalog

	CVE-2022-23748 Dante Discovery Process Control Vulnerability CVE-2024-21413 Microsoft Outlook Improper Input Validation Vulnerability CVE-2020-29574 CyberoamOS (CROS) SQL Injection Vulnerability CVE-2020-15069 Sophos XG Firewall Buffer Overflow Vulnerability CVE-2024-53104 Linux Kernel Out-of-Bounds Write Vulnerability	
CISA Partners with ASD's ACSC, CCCS, NCSC-UK, and Other International and US Organizations to Release Guidance on Edge Devices	network edge devices and appliances, such as firewalls, routers, virtual private networks (VPN) gateways, Internet of Things (IoT) devices, internet-facing servers, and internet-facing operational technology (OT) systems	https://www.cisa.gov/news-events/alerts/2025/02/04/cisa-partners-asds-acsc-cccs-ncsc-uk-and-other-international-and-us-organizations-release-guidance

3 News

Σύντομη περιγραφή / Τίτλος	URL
Zyxel won't patch newly exploited flaws in end-of-life routers	https://www.bleepingcomputer.com/news/security/zyxel-wont-patch-newly-exploited-flaws-in-end-of-life-routers/
Sophos Acquires Secureworks for $859 Million	https://cybersecuritynews.com/sophos-acquires-secureworks-2/
Cybercriminals Weaponize Graphics Files in Phishing Attacks	https://www.infosecurity-magazine.com/news/cybercriminals-graphics-files/
Europol Cracks Down on Global Child Abuse Network "The Com"	https://www.infosecurity-magazine.com/news/europol-cracksdown-child-abuse/
Top 3 Ransomware Threats Active in 2025	https://thehackernews.com/2025/02/top-3-ransomware-threats-active-in-2025.html

3.1 Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Mobile Malware Targeting Indian Banks Exposes 50,000 Users	https://www.infosecurity-magazine.com/news/mobile-malware-indian-banks/
International Civil Aviation Organization (ICAO) and ACAO Breached: Cyberespionage Groups Targeting Aviation Safety Specialists	https://securityaffairs.com/173863/data-breach/icao-and-acao-breached-cyberespionage-groups-targeting-aviation-safety-specialists.html

British engineering firm IMI discloses breach, shares no details	https://www.bleepingcomputer.com/news/security/british-engineering-firm-imi-discloses-breach-shares-no-details/
OpenAI Data Breach: Threat Actor Allegedly Claims 20 Million Logins for Sale	https://cybersecuritynews.com/openai-alleged-data-breach/
DeepSeek's Exposes Full System Prompt in New Jailbreak Method	https://cybersecuritynews.com/deepseeks-exposes-full-system-prompt/

3.2 Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
New Veeam Flaw Allows Arbitrary Code Execution via Man-in-the-Middle Attack	https://thehackernews.com/2025/02/new-veeam-flaw-allows-arbitrary-code.html
7-Zip MotW bypass exploited in zero-day attacks against Ukraine	https://www.bleepingcomputer.com/news/security/7-zip-motw-bypass-exploited-in-zero-day-attacks-against-ukraine/
Chinese Hackers Attacking Linux Devices With New SSH Backdoor	https://cybersecuritynews.com/chinese-hackers-attacking-linux-devices/
Multiple IBM Cloud Pak Vulnerabilities Let Attackers Execute Remote Code	https://cybersecuritynews.com/ibm-cloud-pak-vulnerabilities/
Hackers Exploit GPU Vulnerabilities to Take Complete Control of Your Device	https://cybersecuritynews.com/hackers-could-exploit-gpu-vulnerabilities/
Hackers Exploiting A Six-Year-Old IIS Vulnerability To Gain Remote Access	https://cybersecuritynews.com/hackers-exploiting-a-six-year-old-iis-vulnerability/
0-Day Vulnerabilities in Microsoft Sysinternals Tools Allow Attackers To Launch DLL Injection Attacks on Windows	https://cybersecuritynews.com/0-day-vulnerabilities-in-microsoft-sysinternals-tools/
U.S. CISA adds Microsoft Outlook, Sophos XG Firewall, and other flaws to its Known Exploited Vulnerabilities catalog	https://securityaffairs.com/173949/hacking/u-s-cisa-adds-microsoft-outlook-sophos-xg-firewall-and-other-flaws-to-its-known-exploited-vulnerabilities-catalog.html
Critical RCE bug in Microsoft Outlook now exploited in attacks	https://www.bleepingcomputer.com/news/security/critical-rce-bug-in-microsoft-outlook-now-exploited-in-attacks/
Critical Cisco ISE bug can let attackers run commands as root	https://www.bleepingcomputer.com/news/security/critical-cisco-ise-bug-can-let-attackers-run-commands-as-root/
WordPress ASE Plugin Vulnerability Threatens Site Security	https://www.infosecurity-magazine.com/news/wordpress-ase-plugin-flaw/
CISA: Actively exploited Linux kernel flaw requires immediate remediation	https://www.scworld.com/brief/cisa-actively-exploited-linux-kernel-flaw-requires-immediate-remediation
Cybercrime gang exploited VeraCore zero-day vulnerabilities for years (CVE-2025-25181, CVE-2024-57968)	https://www.helpnetsecurity.com/2025/02/05/cybercrime-exploited-veracore-zero-day-vulnerabilities-cve-2025-25181-cve-2024-57968-xe-group/
F5 BIG-IP SNMP Vulnerability Let Attackers Trigger DoS Attack on System	https://cybersecuritynews.com/f5-big-ip-snmp-vulnerability/
Logsign Vulnerability Remote Attackers to Bypass Authentication	https://cybersecuritynews.com/logsign-vulnerability/
Dell Update Manager Plugin Vulnerability Let Hackers Access Sensitive Data	https://cybersecuritynews.com/dell-update-manager-plugin-vulnerability/
PTZOptics NDI and SDI Cameras Attack	https://www.fortiguard.com/outbreak-alert/ptzoptics-cameras-attack

3.3 Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Netgear urges users to upgrade two flaws impacting WiFi router models	https://securityaffairs.com/173839/security/netgear-wifi-routers-flaws.html
Microsoft shares workaround for Windows security update issues	https://www.bleepingcomputer.com/news/microsoft/microsoft-shares-workaround-for-windows-security-update-issues/
Veeam Updater receives update for critical RCE flaw	https://www.scworld.com/news/veeam-updater-receives-update-for-critical-rce-flaw
AMD fixes bug that lets hackers load malicious microcode patches	https://www.bleepingcomputer.com/news/security/amd-fixes-bug-that-lets-hackers-load-malicious-microcode-patches/
Microsoft Edge Vulnerabilities Let Attackers Execute Remote Code – Update Now!	https://cybersecuritynews.com/edge-vulnerabilities-remote-code/

3.4 Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
Hackers Using HTTP Client Tools To Takeover Microsoft 365 Accounts	https://cybersecuritynews.com/hackers-using-http-client-tools/
CISA Warns of Active Exploits Targeting Trimble Cityworks Vulnerability	https://thehackernews.com/2025/02/cisa-warns-of-active-exploitation-in.html
Attackers compromise IIS servers by leveraging exposed ASP.NET machine keys	https://www.helpnetsecurity.com/2025/02/07/iis-servers-compromised-asp-net-machine-keys-viewstate-code-injection/
Hackers Exploiting SimpleHelp RMM Flaws for Persistent Access and Ransomware	https://thehackernews.com/2025/02/hackers-exploit-simplehelp-rmm-flaws.html
Fake Google Chrome Sites Distribute ValleyRAT Malware via DLL Hijacking	https://thehackernews.com/2025/02/fake-google-chrome-sites-distribute.html
New AsyncRAT campaign uncovered	https://www.scworld.com/brief/new-asyncrat-campaign-uncovered
Ukraine’s largest bank PrivatBank Targeted with SmokeLoader malware	https://hackread.com/ukraine-largest-bank-privatbank-smokeloader-malware/
Banking Malware Uses Live Numbers to Hijack OTPs, Targeting 50,000 Victims	https://hackread.com/banking-malware-live-numbers-hijack-otp-50000-victims/
Novel SSH backdoor leveraged in Chinese cyberespionage attacks	https://www.scworld.com/brief/novel-ssh-backdoor-leveraged-in-chinese-cyberespionage-attacks
Weaponizing Windows Background Images to Gain Admin Access Using AnyDesk Vulnerability	https://cybersecuritynews.com/weaponizing-windows-background-images-to-gain-admin-access/
Hackers Attacking Web Login Pages of Popular Firewalls for Brute-Force Attacks	https://cybersecuritynews.com/hackers-attacking-web-login-pages/

New Attack Technique Uncovered Abusing Kerberos Delegation in Active Directory Networks	https://cybersecuritynews.com/abusing-kerberos-delegation-in-active-directory/

3.5 Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Mastering Linux Monitoring with Tetragon and Wazuh	https://socfortress.medium.com/mastering-linux-monitoring-with-tetragon-and-wazuh-480226881abb
Ghidra 11.3 released: New features, performance improvements, bug fixes	https://www.helpnetsecurity.com/2025/02/07/ghidra-11-3-released-new-features-performance-improvements-bug-fixes/
New infosec products of the week: February 7, 2025	https://www.helpnetsecurity.com/2025/02/07/new-infosec-products-of-the-week-february-7-2025/
OpenNHP: Cryptography-driven zero trust protocol	https://www.helpnetsecurity.com/2025/02/05/opennhp-cryptography-driven-zero-trust-protocol/
11 Open Source Cloud Security Tools 2025	https://cybersecuritynews.com/opensource-cloud-security-tools/
Splunk Unveils a New AI Based Honeypot “DECEIVE” to Log Attacker Activities	https://cybersecuritynews.com/splunk-ai-based-honeypot-deceive/

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.

5 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/