Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: DD/MM/YYYY - DD/MM/YYYY

Contents

Common Vulnerabilities and Exposures (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-2025-2619	**9,8**	D-Link DAP-1620	**Improper Restriction of Operations within the Bounds of a Memory Buffer**	D-Link DAP-1620 1.03	n/a	https://vuldb.com/?ctiid.300621 https://vuldb.com/?id.300621 https://vuldb.com/?submit.518968 https://witty-maiasaura-083.notion.site/D-link-DAP-1620-check_dws_cookie-Vulnerability-1b4b2f2a6361805ca74fdf4949385ade https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-2618	**9,8**	D-Link DAP-1620	**Improper Restriction of Operations within the Bounds of a Memory Buffer**	D-Link DAP-1620 1.03	n/a	https://vuldb.com/?ctiid.300620 https://vuldb.com/?id.300620 https://vuldb.com/?submit.518963 https://witty-maiasaura-083.notion.site/D-link-DAP-1620-set_ws_action-Vulnerability-1afb2f2a6361804e86dcde1e78ea2a8e https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-29814	**9,3**	Microsoft Partner Center	**Improper Input Validation**		n/a	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29814
https://nvd.nist.gov/vuln/detail/CVE-2025-29927	**9,1**	Next.js	**Improper Authorization**	Prior to 14.2.25 and 15.2.3	n/a	http://www.openwall.com/lists/oss-security/2025/03/23/3 http://www.openwall.com/lists/oss-security/2025/03/23/4 https://github.com/vercel/next.js/security/advisories/GHSA-f82v-jwr5-mffw
https://nvd.nist.gov/vuln/detail/CVE-2025-30472	**9**	Corosync	**Stack-based Buffer Overflow**	Corosync through 3.1.9	n/a	https://corosync.org https://github.com/corosync/corosync/blob/73ba225cc48ebb1903897c792065cb5e876613b0/exec/totemsrp.c#L4677 https://github.com/corosync/corosync/issues/778
https://nvd.nist.gov/vuln/detail/CVE-2025-0724	**8,8**	The ProfileGrid – User Profiles, Groups and Communities plugin for WordPress	**Deserialization of Untrusted Data**	PHP Object Injection in all versions up to, and including, 5.9.4.5	n/a	https://plugins.trac.wordpress.org/browser/profilegrid-user-profiles-groups-and-communities/tags/5.9.4.2/includes/class-profile-magic-html-generator.php#L259 https://www.wordfence.com/threat-intel/vulnerabilities/id/6bb1de69-7bc2-4785-9789-0a2d1cf35b9b?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-2303	**8,8**	The Block Logic – Full Gutenberg Block Display Control plugin for WordPress	**Improper Control of Generation of Code ('Code Injection')**	Remote Code Execution in all versions up to, and including, 1.0.8	n/a	https://plugins.trac.wordpress.org/browser/block-logic/tags/1.0.8/block-logic.php#L127 https://www.wordfence.com/threat-intel/vulnerabilities/id/4a76f851-3f4e-4457-a33c-eede51c4b4d1?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-29230	**8,6**	Linksys E5600	**Improper Neutralization of Special Elements used in a Command ('Command Injection')**	Linksys E5600 v1.1.0.26	n/a	https://github.com/JZP018/Vuln/blob/main/linsys/E5600/CI_emailReg_email/CI_emailReg_email.md
https://nvd.nist.gov/vuln/detail/CVE-2025-2609	**8,2**	MagnusSolution MagnusBilling login	**Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')**	MagnusBilling: through 7.3.0.	n/a	https://chocapikk.com/posts/2025/magnusbilling/ https://github.com/magnussolution/magnusbilling7/commit/f0f083c76157e31149ae58342342fb1bf1629e22 https://vulncheck.com/advisories/magnusbilling-logs-xss
https://nvd.nist.gov/vuln/detail/CVE-2025-2691	**8,2**	The web server	**Server-Side Request Forgery (SSRF)**	Versions of the package nossrf before 1.0.4 are vulnerable to Server-Side Request Forgery (SSRF)	n/a	https://security.snyk.io/vuln/SNYK-JS-NOSSRF-9510842
https://nvd.nist.gov/vuln/detail/CVE-2025-0927	**7,8**	the HFS+ file system implementation in the Linux Kernel	**Out-of-bounds Write**	the HFS+ file system implementation in the Linux Kernel	n/a	https://ubuntu.com/security/CVE-2025-0927 https://ubuntu.com/security/notices/USN-7276-1
https://nvd.nist.gov/vuln/detail/CVE-2025-29795	**7,8**	Microsoft Edge	**Improper Link Resolution Before File Access ('Link Following')**	Microsoft Edge (Chromium-based)	n/a	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29795
https://nvd.nist.gov/vuln/detail/CVE-2025-24915	**7,8**	Nessus Agent	**Incorrect Default Permissions**	versions prior to 10.8.3	n/a	https://www.tenable.com/security/tns-2025-02

https://nvd.nist.gov/vuln/detail/CVE-2025-2610	**7,6**	MagnusSolution MagnusBilling	**Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')**	MagnusBilling: through 7.3.0.	n/a	https://chocapikk.com/posts/2025/magnusbilling/ https://github.com/magnussolution/magnusbilling7/commit/f0f083c76157e31149ae58342342fb1bf1629e22 https://vulncheck.com/advisories/magnusbilling-alarm-xss
https://nvd.nist.gov/vuln/detail/CVE-2025-30204	**7,5**	JSON Web Tokens	**Asymmetric Resource Consumption (Amplification)**	JSON Web Tokens. Prior to 5.2.2 and 4.5.2	n/a	https://github.com/golang-jwt/jwt/security/advisories/GHSA-mh63-6h87-95cp
https://nvd.nist.gov/vuln/detail/CVE-2025-2640	**7,5**	PHPGurukul Doctor Appointment Management System	**Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')**	PHPGurukul Doctor Appointment Management System 1.0	n/a	https://github.com/AiENG07/CVE/issues/1 https://phpgurukul.com/ https://vuldb.com/?ctiid.300641 https://vuldb.com/?id.300641 https://vuldb.com/?submit.519644
https://nvd.nist.gov/vuln/detail/CVE-2025-25068	**7,5**	Mattermost	**Missing Authentication for Critical Function**	Mattermost versions 10.4.x <= 10.4.2, 10.3.x <= 10.3.3, 9.11.x <= 9.11.8, 10.5.x <= 10.5.0	n/a	https://mattermost.com/security-updates
https://nvd.nist.gov/vuln/detail/CVE-2025-30204	**7,5**	golang-jwt	**Asymmetric Resource Consumption (Amplification)**	Prior to 5.2.2 and 4.5.2	n/a	https://github.com/golang-jwt/jwt/commit/0951d184286dece21f73c85673fd308786ffe9c3 https://github.com/golang-jwt/jwt/security/advisories/GHSA-mh63-6h87-95cp
https://nvd.nist.gov/vuln/detail/CVE-2025-2683	**7,3**	PHPGurukul Bank Locker Management System	**Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')**	PHPGurukul Bank Locker Management System 1.0	n/a	https://github.com/ARPANET-cyber/CVE/issues/12 https://phpgurukul.com/ https://vuldb.com/?ctiid.300700 https://vuldb.com/?id.300700 https://vuldb.com/?submit.521452
https://nvd.nist.gov/vuln/detail/CVE-2025-2684	**7,3**	PHPGurukul Bank Locker Management System	**Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')**	PHPGurukul Bank Locker Management System 1.1	n/a	https://github.com/ARPANET-cyber/CVE/issues/13 https://phpgurukul.com/ https://vuldb.com/?ctiid.300701 https://vuldb.com/?id.300701 https://vuldb.com/?submit.521453

https://nvd.nist.gov/vuln/detail/CVE-2025-2643	**7,3**	PHPGurukul Art Gallery Management System	**Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')**	PHPGurukul Art Gallery Management System 1.0	n/a	https://github.com/liuhao2638/cve/issues/6 https://phpgurukul.com/ https://vuldb.com/?ctiid.300658 https://vuldb.com/?id.300658 https://vuldb.com/?submit.519772
https://nvd.nist.gov/vuln/detail/CVE-2025-2654	**7,3**	SourceCodester AC Repair and Services System	**Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')**	SourceCodester AC Repair and Services System 1.0	n/a	https://github.com/Colorado-all/cve/blob/main/AC%20Repair%20and%20Services%20System%20using/SQL-4.md https://vuldb.com/?ctiid.300669 https://vuldb.com/?id.300669 https://vuldb.com/?submit.520013 https://www.sourcecodester.com/
https://nvd.nist.gov/vuln/detail/CVE-2025-2655	**7,3**	SourceCodester AC Repair and Services System	**Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')**	SourceCodester AC Repair and Services System 1.0	n/a	https://github.com/Colorado-all/cve/blob/main/AC%20Repair%20and%20Services%20System%20using/SQL-8.md
https://nvd.nist.gov/vuln/detail/CVE-2025-2656	**7,3**	PHPGurukul Zoo Management System	**Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')**	PHPGurukul Zoo Management System 2.1	n/a	
https://nvd.nist.gov/vuln/detail/CVE-2025-2657	**7,3**	Apartment Visitors Management System	**Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')**	Apartment Visitors Management System 1.0.	n/a	https://github.com/ydnd/cve/issues/5 https://vuldb.com/?ctiid.300673 https://vuldb.com/?id.300673 https://vuldb.com/?submit.520237
https://nvd.nist.gov/vuln/detail/CVE-2025-2658	**7,3**	PHPGurukul Online Security Guards Hiring System	**Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')**	PHPGurukul Online Security Guards Hiring System 1.0	n/a	https://github.com/zyb26252/CVE/issues/1 https://phpgurukul.com/ https://vuldb.com/?ctiid.300674 https://vuldb.com/?id.300674 https://vuldb.com/?submit.520250
https://nvd.nist.gov/vuln/detail/CVE-2025-2660	**7,3**	Project Worlds Online Time Table Generator	**Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')**	Project Worlds Online Time Table Generator 1.0	n/a	https://github.com/ydnd/cve/issues/8 https://vuldb.com/?ctiid.300676 https://vuldb.com/?id.300676 https://vuldb.com/?submit.520483

https://nvd.nist.gov/vuln/detail/CVE-2025-2661	**7,3**	Project Worlds Online Time Table Generator	**Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')**	Project Worlds Online Time Table Generator 1.0	n/a	https://github.com/ydnd/cve/issues/9 https://vuldb.com/?ctiid.300677 https://vuldb.com/?id.300677 https://vuldb.com/?submit.520484
https://nvd.nist.gov/vuln/detail/CVE-2025-2676	**7,3**	PHPGurukul Bank Locker Management System	**Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')**	PHPGurukul Bank Locker Management System 1.0	n/a	https://github.com/ARPANET-cyber/CVE/issues/5 https://phpgurukul.com/ https://vuldb.com/?ctiid.300693 https://vuldb.com/?id.300693 https://vuldb.com/?submit.521443
https://nvd.nist.gov/vuln/detail/CVE-2025-25035	**7,3**	Jalios JPlatform 10	**Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')**	JPlatform 10: before 10.0.8 (SP8), before 10.0.7 (SP7), before 10.0.6 (SP6) and Jalios Workplace 6.2, Jalios Workplace 6.1, Jalios Workplace 6.0, and Jalios Workplace 5.3 to 5.5	n/a	https://community.jalios.com/jcms/jc1_893720/en/security-alert-2025-02-19 https://issues.jalios.com/browse/JCMS-11246 https://issues.jalios.com/browse/JCMS-11248 https://issues.jalios.com/browse/JCMS-11259 https://vulncheck.com/advisories/jalios-jplatform-xss

https://nvd.nist.gov/vuln/detail/CVE-2025-30349	**7,2**	Horde IMP	**Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')**	6.2.27, as used with Horde Application Framework through 5.2.23	n/a	https://github.com/horde/base/releases/tag/v5.2.23 https://github.com/horde/imp/blob/fd9212ca3b72ff834504af4886f7d95138619bd4/doc/INSTALL.rst?plain=1#L23-L25 https://github.com/horde/imp/blob/fd9212ca3b72ff834504af4886f7d95138619bd4/doc/INSTALL.rst?plain=1#L61-L62 https://github.com/horde/imp/releases/tag/v6.2.27 https://github.com/horde/webmail/releases/tag/v5.2.22 https://lists.horde.org/archives/imp/Week-of-Mon-20250317/057781.html https://lists.horde.org/archives/imp/Week-of-Mon-20250317/057784.html https://web.archive.org/web/20250321152616/https://lists.horde.org/archives/imp/Week-of-Mon-20250317/057781.html https://web.archive.org/web/20250321162434/https://lists.horde.org/archives/imp/Week-of-Mon-20250317/057784.html https://www.horde.org/apps/horde https://www.horde.org/apps/imp https://www.horde.org/download/horde

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Releases Five Industrial Control Systems Advisories	▪ **ICSA-25-079-01** Schneider Electric EcoStruxure™ ▪ **ICSA-25-079-02** Schneider Electric Enerlin'X IFE and eIFE ▪ **ICSA-25-079-03** Siemens Simcenter Femap ▪ **ICSA-25-079-04** SMA Sunny Portal	**https://www.cisa.gov/news-events/alerts/2025/03/20/cisa-releases-five-industrial-control-systems-advisories**
Santesoft Sante DICOM Viewer Pro	**CVE-2025-2480**	**https://www.cisa.gov/news-events/ics-medical-advisories/icsma-25-079-01**

News

Σύντομη περιγραφή / Τίτλος	URL
Get $5000: GitHub Dorks & Leaks	**https://infosecwriteups.com/get-5000-github-dorks-leaks-b26728099d38?source=collection_home**
Attackers Use Fake CAPTCHAs to Deploy Lumma Stealer RAT	**https://www.infosecurity-magazine.com/news/attackers-fake-captchas-lumma/**
NAKIVO Backup & Replication vulnerability exploited by attackers (CVE-2024-48248)	**https://www.helpnetsecurity.com/2025/03/21/nakivo-backup-replication-vulnerability-exploited-by-attackers-cve-2024-48248/**
Microsoft Trusted Signing service abused to code-sign malware	**https://www.bleepingcomputer.com/news/security/microsoft-trusted-signing-service-abused-to-code-sign-malware/**
Security Affairs newsletter Round 516 by Pierluigi Paganini – INTERNATIONAL EDITION	**https://securityaffairs.com/175740/breaking-news/security-affairs-newsletter-round-516-by-pierluigi-paganini-international-edition.html**
FBI warnings are true—fake file converters do push malware	**https://www.bleepingcomputer.com/news/security/fbi-warnings-are-true-fake-file-converters-do-push-malware/**
How Cybercriminals Exploit Notification Channels	**https://hackread.com/how-cybercriminals-exploit-notification-channels/**
How Cybercriminals Exploit Public Info for Attacks: Understanding Risks and Prevention	**https://hackread.com/how-cybercriminals-exploit-public-info-attacks-risks-prevention/**
Cloudflare now blocks all unencrypted traffic to its API endpoints	**https://www.bleepingcomputer.com/news/security/cloudflare-now-blocks-all-unencrypted-traffic-to-its-api-endpoints/**
Oracle Denies Breach Amid Hacker's Claim of Access to 6 Million Records	**https://hackread.com/oracle-denies-breach-hacker-access-6-million-records/**

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL
Cloak ransomware group hacked the Virginia Attorney General's Office	**https://securityaffairs.com/175751/data-breach/cloak-group-hacked-virginia-attorney-generals-office.html**
Coinbase Initially Targeted in GitHub Actions Supply Chain Attack; 218 Repositories' CI/CD Secrets Exposed	**https://thehackernews.com/2025/03/github-supply-chain-breach-coinbase.html**

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Zero-day broker Operation Zero offers up to $4 million for Telegram exploits	https://securityaffairs.com/175709/hacking/operation-zero-offers-4m-for-telegram-exploits.html
Checkpoint ZoneAlarm Driver Flaw Exposes Users to Credential Theft	https://hackread.com/checkpoint-zonealarm-driver-flaw-user-credential-theft/
New Attacks Exploit Year-Old ServiceNow Flaws – Israel Hit Hardest	https://hackread.com/attacks-exploit-servicenow-flaws-israel-hit-hardest/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
North Korea Launches New Military Based Research Center To Strengthen Hacking Capabilities	https://cybersecuritynews.com/north-korea-launches-new-military-based-research-center/
VMware Vulnerabilities Exploited Actively to Bypass Security Controls & Deploy Ransomware	https://cybersecuritynews.com/vmware-vulnerabilities-exploited-ransomware/
Hacker Claims Sale of 6 Million Records Stolen from Oracle Cloud Servers	https://cybersecuritynews.com/hacker-claims-6-million-oracle-records/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Top 10 Best Cyber Attack Simulation Tools – 2025	https://cybersecuritynews.com/cyber-attack-simulation-tools/
Top Cybersecurity Tools of 2025 To Managing Remote Device Threats	https://cybersecuritynews.com/top-cybersecurity-tools-managing-remote-device-threats/

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/