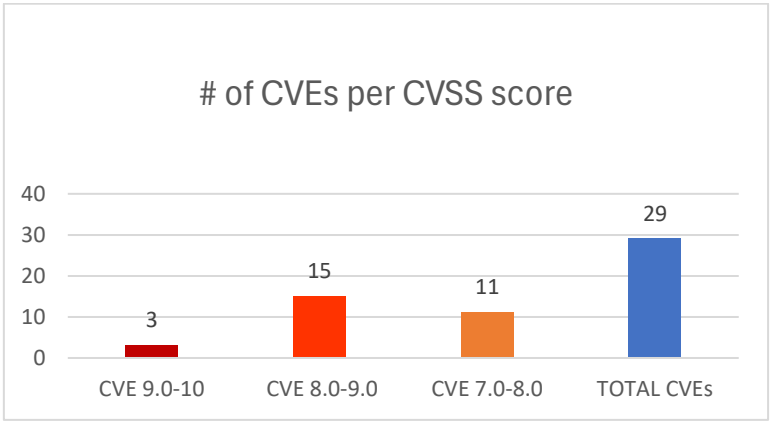
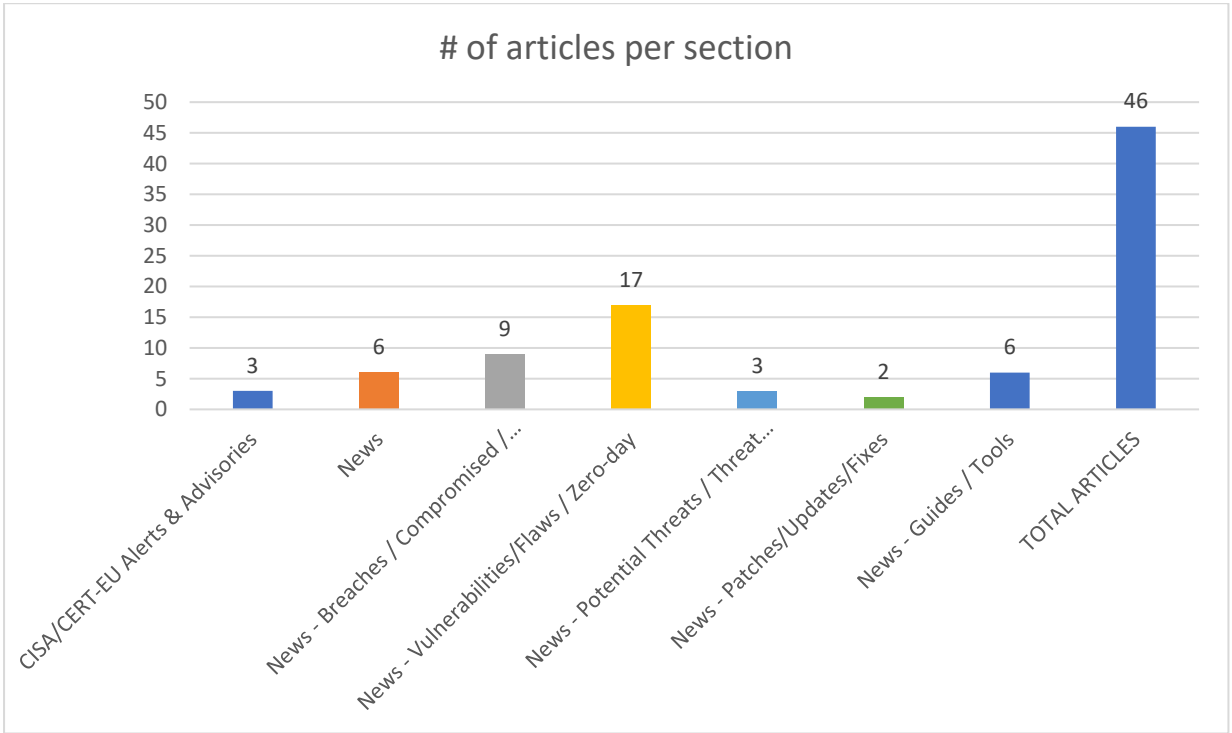
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 03/12/2025 - 05/12/2025





Contents

Common Vulnerabilities and Exposures (CVEs)

Η ενότητα αυτή εστιάζει σε ευπάθειες που έχουν καταχωρηθεί πρόσφατα και αξιολογούνται ως σοβαρές, με βάση τη βαθμολογία CVSS. Παρουσιάζονται με σαφήνεια τα συστήματα ή εφαρμογές που επηρεάζονται, ο τύπος της ευπάθειας (όπως SQL injection ή command injection) και σχετικοί σύνδεσμοι για περαιτέρω πληροφόρηση ή μέτρα αντιμετώπισης.

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-2025-66570	10,0	cpp-httplib	Insufficient Verification of Data Authenticity	Prior to 0.27.0	https://github.com/yhirose/cpp-httplib/commit/ac9ebb0ee333ce8bf13523f487bdfad9518a2aff GitHub, Inc. https://github.com/yhirose/cpp-httplib/security/advisories/GHSA-xm2j-vfr9-mg9m
https://nvd.nist.gov/vuln/detail/CVE-2025-12374	9,8	The Email Verification, Email OTP, Block Spam Email, Passwordless login, Hide Login, Magic Login – User Verification plugin for WordPress	Improper Authentication	up to, and including, 2.0.39	https://plugins.trac.wordpress.org/browser/user-verification/trunk/templates/email-otp-login-form/hook.php#L141 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/8ccb1304-326e-43af-b75d-23874f92ba8b?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-13313	9,8	The CRM Memberships plugin for WordPress	Missing Authorization	up to, and including, 2.5	https://plugins.trac.wordpress.org/browser/crm-memberships/tags/2.5/includes/class/class-ntzcrm-api.php#L12 Wordfence https://plugins.trac.wordpress.org/browser/crm-memberships/tags/2.5/includes/class/class-ntzcrm-api.php#L63 Wordfence https://plugins.trac.wordpress.org/browser/crm-memberships/tags/2.5/includes/class/class-ntzcrm-api.php#L795 Wordfence https://plugins.trac.wordpress.org/browser/crm-memberships/tags/2.5/includes/class/class-ntzcrm-dbquery.php#L287 Wordfence https://plugins.trac.wordpress.org/browser/crm-memberships/tags/2.5/ntzcrm-memberships.php#L42 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/e2837399-c44f-494e-bdc6-f9c6e4e2dc11?source=cve

https://nvd.nist.gov/vuln/detail/CVE-2025-65897	8,8	zdh_web	Unrestricted Upload of File with Dangerous Type	zdh_web thru 5.6.17	https://github.com/zhaoyachao/zdh_web MITRE https://github.com/zhaoyachao/zdh_web/commit/b2423378a8bf83f159f19ce4e14eac71c939793a MITRE https://github.com/zhaoyachao/zdh_web/issues/40 MITRE https://github.com/zhaoyachao/zdh_web/pull/39
https://nvd.nist.gov/vuln/detail/CVE-2025-12181	8,8	The ContentStudio plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 1.3.7	https://wordpress.org/plugins/contentstudio/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/5b92b0a4-7ebf-43b3-837b-ad710e5e35ff?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-12154	8,8	The Auto Thumbnailer plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 1.0	https://wordpress.org/plugins/auto-thumbnailer/ Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/d7c98191-bf17-4e94-88cc-ad385b1fe97d?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-13066	8,8	The Demo Importer Plus plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 2.0.6	https://plugins.trac.wordpress.org/changeset/3400301/demo-importer-plus/trunk/inc/importers Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/7df0ea8a-5e2c-4f5e-a326-b92df37ffa3c?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-13543	8,8	The PostGallery plugin for WordPress	Unrestricted Upload of File with Dangerous Type	up to, and including, 1.12.5	https://plugins.trac.wordpress.org/browser/postgallery/tags/1.12.5/admin/PostGalleryUploader.php Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/13348eb5-5001-4ec4-bc6a-44795bbed203?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-14015	8,8	H3C Magic B0	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	up to 100R002	https://github.com/HungryGoogle/log_attack/blob/main/index2/2.md CISA-ADP, VulDB https://vuldb.com/?ctiid.334256 VulDB https://vuldb.com/?id.334256 VulDB https://vuldb.com/?submit.694755
https://nvd.nist.gov/vuln/detail/CVE-2025-66287	8,8	WebKitGTK	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')		https://access.redhat.com/errata/RHSA-2025:22789 Red Hat, Inc. https://access.redhat.com/errata/RHSA-2025:22790 Red Hat, Inc. https://access.redhat.com/security/cve/CVE-2025-66287 Red Hat, Inc. https://bugzilla.redhat.com/show_bug.cgi?id=2418857 Red Hat, Inc. https://webkitgtk.org/security/WSA-2025-0009.html

https://nvd.nist.gov/vuln/detail/CVE-2025-65959	8,7	Open WebUI	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Prior to 0.6.37	https://github.com/open-webui/open-webui/commit/03cc6ce8eb5c055115406e2304fbf7e3338b8dce GitHub, Inc. https://github.com/open-webui/open-webui/security/advisories/GHSA-8wvc-869r-xfqf
https://nvd.nist.gov/vuln/detail/CVE-2025-65036	8,3	XWiki Remote Macros	Missing Authorization	Prior to 1.27.1	https://github.com/xwikisas/xwiki-pro-macros/security/advisories/GHSA-472x-fwh9-r82f
https://nvd.nist.gov/vuln/detail/CVE-2025-58098	8,3	Apache HTTP Server	Insertion of Sensitive Information Into Sent Data	2.4.65 and earlier	http://www.openwall.com/lists/oss-security/2025/12/04/5 CVE https://httpd.apache.org/security/vulnerabilities_24.html
https://nvd.nist.gov/vuln/detail/CVE-2025-64053	8,2	Fanvil	Stack-based Buffer Overflow	x210 2.12.20	http://fanvil.com MITRE https://github.com/SpikeReply/advisories/blob/main/cve/fanvil/cve-2025-64053.md
https://nvd.nist.gov/vuln/detail/CVE-2025-65879	8,1	Warehouse Management System	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	1.2	https://github.com/W000i/vuln/issues/3
https://nvd.nist.gov/vuln/detail/CVE-2025-13614	8,1	The Cool Tag Cloud plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 2.29	http://plugins.trac.wordpress.org/browser/cool-tag-cloud/trunk/cool-tag-cloud.php?marks=798-799#L682 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/eac56190-4f81-464d-9737-ae2e3d4b0d0d?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-12851	8,1	The My auctions allegro plugin for WordPress	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion)	up to, and including, 3.6.32	https://plugins.trac.wordpress.org/changeset/3402268/my-auctions-allegro-free-edition Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/202a8493-6df0-4a5e-b6bf-099219830e01?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-12995	8,1	Medtronic CareLink Network	Improper Restriction of Excessive Authentication Attempts	CareLink Network: before	https://www.medtronic.com/en-us/e/product-security/security-bulletins/carelink-network-vulnerabilities.html

				December 4, 2025	
https://nvd.nist.gov/vuln/detail/CVE-2024-9183	7,7	GitLab	Time-of-check Time-of-use (TOCTOU) Race Condition	from 18.4 prior to 18.4.5, 18.5 prior to 18.5.3, and 18.6 prior to 18.6.1	https://gitlab.com/gitlab-org/gitlab/-/issues/494478 GitLab Inc. https://hackerone.com/reports/2707421
https://nvd.nist.gov/vuln/detail/CVE-2025-66624	7,5	BACnet Protocol Stack library	Out-of-bounds Read	Prior to 1.5.0.rc2	https://github.com/bacnet-stack/bacnet-stack/commit/9378f7d1e70169ebde4a5090bae7603703eadf48 GitHub, Inc. https://github.com/bacnet-stack/bacnet-stack/security/advisories/GHSA-8wgw-5h6x-qgqg
https://nvd.nist.gov/vuln/detail/CVE-2025-12850	7,5	The My auctions allegro plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	up to, and including, 3.6.32	https://plugins.trac.wordpress.org/changeset/3402268/my-auctions-allegro-free-edition Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/dc4883b8-5783-49ff-ab3b-c568c9923227?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2025-66506	7,5	Fulcio is a free-to-use certificate authority	Asymmetric Resource Consumption (Amplification)	Prior to 1.8.3	https://github.com/sigstore/fulcio/commit/765a0e57608b9ef390e1eeeea8595b9054c63a5a GitHub, Inc. https://github.com/sigstore/fulcio/security/advisories/GHSA-f83f-xpx7-ffpw
https://nvd.nist.gov/vuln/detail/CVE-2025-56427	7,5	ComposioHQ	Exposure of Sensitive Information to an Unauthorized Actor	v.0.7.20	https://github.com/ComposioHQ/composio/blob/master/python/composio/server/api.py#L278 MITRE https://github.com/TOAST-Research/pocs/blob/main/composio/composio_1.md
https://nvd.nist.gov/vuln/detail/CVE-2025-57210	7,5	ApiPayController.java	Improper Access Control	v1.0.0	https://gist.github.com/xueye0629/4411663241fa3bbba628d3044dc50451 MITRE Third Party Advisory https://gitee.com/fuyang_lipengjun/platform

https://nvd.nist.gov/vuln/detail/CVE-2025-63363	7,5	Waveshare RS232/485 TO WIFI ETH (B) Serial to Ethernet/Wi-Fi Gateway	Improper Access Control	Firmware V3.1.1.0: HW 4.3.2.1: Webpage V7.04T.07.002880.0301	https://drive.google.com/file/d/1AGv9KWMTB71NJflOn-cuNO6FyK0UAqxmL/view?usp=sharing MITRE https://otsecverse.github.io/OTSecVerse/posts/Post-3/
https://nvd.nist.gov/vuln/detail/CVE-2025-54159	7,5	BeeDrive in Synology	Missing Authorization	before 1.4.2-13960	https://www.synology.com/en-global/security/advisory/Synology_SA_25_08
https://nvd.nist.gov/vuln/detail/CVE-2025-66561	7,3	SysReptor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Prior to 2025.102	https://github.com/Syslifters/sysreptor/security/advisories/GHSA-64vw-v5c4-mgvm
https://nvd.nist.gov/vuln/detail/CVE-2025-66238	7,2	DCIM dcTrack	Authentication Bypass Using an Alternate Path or Channel		https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2025/icsa-25-338-05.json ICS-CERT https://www.cisa.gov/news-events/ics-advisories/icsa-25-338-05
https://nvd.nist.gov/vuln/detail/CVE-2025-46603	7,0	Dell CloudBoost Virtual Appliance	Improper Restriction of Excessive Authentication Attempts	19.13.0.0 and prior	https://www.dell.com/support/kbdoc/en-us/000397417/dsa-2025-387-security-update-for-dell-cloudboost-virtual-appliance-multiple-vulnerabilities

CISA/CERT-EU Alerts & Advisories

Αυτό το κομμάτι περιλαμβάνει ειδοποιήσεις από επίσημες πηγές, κυρίως CISA και CERT-EU, σχετικά με κρίσιμες ευπάθειες ή ενεργές απειλές. Συνήθως αφορούν βιομηχανικά ή κρίσιμα συστήματα, αλλά και mainstream λογισμικό. Προσφέρονται σε μορφή σύντομων αναφορών και οδηγούν σε πιο λεπτομερείς τεχνικές οδηγίες.

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Releases Nine Industrial Control Systems Advisories	▪ **ICSA-25-338-01** Mitsubishi Electric GX Works2 ▪ **ICSA-25-338-02** MAXHUB Pivot ▪ **ICSA-25-338-03** Johnson Controls OpenBlue Mobile Web Application for OpenBlue Workplace ▪ **ICSA-25-338-04** Johnson Controls iSTAR ▪ **ICSA-25-338-05** Sunbird DCIM dcTrack and Power IQ ▪ **ICSA-25-338-06** SolisCloud Monitoring Platform ▪ **ICSA-25-338-07** Advantech iView ▪ **ICSA-25-148-03** Consilium Safety CS5000 Fire Panel (Update A) ▪ **ICSA-25-219-02** Johnson Controls FX Server, FX80 and FX90 (Update A)	https://www.cisa.gov/news-events/alerts/2025/12/04/cisa-releases-nine-industrial-control-systems-advisories
BRICKSTORM Backdoor		https://www.cisa.gov/news-events/analysis-reports/ar25-338a
PRC State-Sponsored Actors Use BRICKSTORM Malware Across Public Sector and Information Technology Systems		https://www.cisa.gov/news-events/alerts/2025/12/04/prc-state-sponsored-actors-use-brickstorm-malware-across-public-sector-and-information-technology

News

Η ενότητα "News" συνοψίζει τα πιο σημαντικά γεγονότα της εβδομάδας στον τομέα της κυβερνοασφάλειας. Εδώ θα βρείτε επιθέσεις που ξεχώρισαν, νέες τεχνικές που εντοπίστηκαν, ή ενέργειες από γνωστές ομάδες hacking. Δίνει την απαραίτητη εικόνα του τι συμβαίνει διεθνώς και πού πρέπει να στραφεί η προσοχή.

Σύντομη περιγραφή / Τίτλος	URL
CISA Publishes Security Guidance for Using AI in OT	https://www.darkreading.com/cybersecurity-operations/cisa-publishes-security-guidance-ai-ot
'MuddyWater' Hackers Target Israeli Orgs With Retro Game Tactic	https://www.darkreading.com/threat-intelligence/muddywater-hackers-israeli-orgs-retro-game
CISA and International Partners Issue Guidance for Secure AI in Infrastructure	https://www.infosecurity-magazine.com/news/us-guidance-secure-ai-ot/
New GhostFrame Phishing Framework Hits Over One Million Attacks	https://www.infosecurity-magazine.com/news/ghostframe-phishing-hits-one/

UK's Cyber Service for Telcos Blocks One Billion Malicious Site Attempts	https://www.infosecurity-magazine.com/news/uk-cyber-service-blocks-billion/
Skills Shortages Trump Headcount as Critical Cyber Challenge	https://www.infosecurity-magazine.com/news/skills-shortages-headcount-2025/

Breaches / Compromised / Hacked

Καταγράφονται περιπτώσεις παραβίασης δεδομένων, διαρροών και άλλων σοβαρών περιστατικών ασφαλείας. Περιλαμβάνονται πληροφορίες για το ποιοι επηρεάστηκαν, με ποιον τρόπο έγινε η παραβίαση και πού υπάρχουν διαθέσιμες λεπτομέρειες. Είναι μια χρήσιμη εικόνα για να αντιληφθεί κανείς τη δυναμική των επιθέσεων σε πραγματικές συνθήκες.

Σύντομη περιγραφή / Τίτλος	URL
Yearn Finance yETH Pool Hit by $9M Exploit	https://www.infosecurity-magazine.com/news/yearn-finance-yeth-pool-exploit/
Post Office Escapes £1m Fine After Postmaster Data Breach	https://www.infosecurity-magazine.com/news/post-office-1m-fine-postmaster/
Freedom Mobile discloses data breach exposing customer data	https://www.bleepingcomputer.com/news/security/freedom-mobile-discloses-data-breach-exposing-customer-data/?&web_view=true
Ransomware gang demands sheriff of Cleveland County, OK pay almost $800,000 in one week	https://www.comparitech.com/news/ransomware-gang-demands-sheriff-of-cleveland-county-ok-pay-almost-800000-in-one-week?&web_view=true
SEEDSNATCHER Android Malware Attacking Users to Exfiltrate Sensitive Data and Execute Malicious Commands	https://cybersecuritynews.com/seedsnatcher-android-malware-attacking-users/
Threat Actors Leveraging Foxit PDF Reader to Gain System Control and Steal Sensitive Data	https://cybersecuritynews.com/threat-actors-leveraging-foxit-pdf-reader/
Freedom Mobile Data Breach Exposes Personal Information of Customers	https://cybersecuritynews.com/freedom-mobile-data-breach/
29.7 Tbps DDoS Attack Via Aisuru Botnet Breaks Internet With New World Record	https://cybersecuritynews.com/29-7-tbps-ddos-attack/
Shai-Hulud 2.0 Malware Attack Compromised 30,000 Repositories and Stolen 500 GitHub Usernames and Tokens	https://cybersecuritynews.com/shai-hulud-2-0-malware-attack-compromised-30000-repositories/

Vulnerabilities / Flaws / Zero-day

Αναφέρονται τεχνικά ελαττώματα ή αδυναμίες που ενδέχεται να αξιοποιηθούν άμεσα από επιτιθέμενους — είτε επειδή είναι zero-day είτε γιατί η διόρθωσή τους καθυστερεί. Περιλαμβάνονται περιπτώσεις όπου δεν απαιτείται αλληλεπίδραση με τον χρήστη ή όπου παρακάμπτονται βασικά μέτρα ασφαλείας. Πολύ χρήσιμο για ομάδες που ασχολούνται με threat detection.

Σύντομη περιγραφή / Τίτλος	URL
JPCERT Confirms Active Command Injection Attacks on Array AG Gateways	https://thehackernews.com/2025/12/jpcert-confirms-active-command.html
Chinese Hackers Exploiting React2Shell Vulnerability	https://www.securityweek.com/chinese-hackers-exploiting-react2shell-vulnerability/

React2Shell: In-the-Wild Exploitation Expected for Critical React Vulnerability	https://www.securityweek.com/react2shell-in-the-wild-exploitation-expected-for-critical-react-vulnerability/
Microsoft Silently Mitigated Exploited LNK Vulnerability	https://www.securityweek.com/microsoft-silently-mitigated-exploited-lnk-vulnerability/
Critical King Addons Vulnerability Exploited to Hack WordPress Sites	https://www.securityweek.com/critical-king-addons-vulnerability-exploited-to-hack-wordpress-sites/
Critical React Flaw Triggers Calls for Immediate Action	https://www.darkreading.com/vulnerabilities-threats/critical-react-flaw-triggers-immediate-action
Hackers are exploiting ArrayOS AG VPN flaw to plant webshells	https://www.bleepingcomputer.com/news/security/hackers-are-exploiting-arrayos-ag-vpn-flaw-to-plant-webshells/
Critical React, Next.js flaw lets hackers execute code on servers	https://www.bleepingcomputer.com/news/security/critical-react2shell-flaw-in-react-nextjs-lets-hackers-run-javascript-code/
Cacti Command Injection Vulnerability Let Attackers Execute Malicious Code Remotely	https://cybersecuritynews.com/cacti-command-injection-vulnerability/
Splunk Enterprise Vulnerabilities Allows Privileges Escalation Via Incorrect File Permissions	https://cybersecuritynews.com/splunk-enterprise-permission-vulnerabilities/
PoC Exploit Released for Critical React, Next.js RCE Vulnerability (CVE-2025-55182)	https://cybersecuritynews.com/poc-exploit-react-next-js/
Prompt Injection Flaw in GitHub Actions Hits Fortune 500 Firms	https://cybersecuritynews.com/prompt-injection-github-actions/
CISA Warns of OpenPLC ScadaBR File Upload Vulnerability Exploited in Attacks	https://cybersecuritynews.com/cisa-warns-of-openplc-scadabr-file-upload-vulnerability-exploited-in-attacks/
PickleScan 0-Day Vulnerabilities Enable Arbitrary Code Execution via Malicious PyTorch Models	https://cybersecuritynews.com/picklescan-0-day-vulnerabilities/
Vim for Windows Vulnerability Let Attackers Execute Arbitrary Code	https://cybersecuritynews.com/vim-windows-vulnerability/
Longwatch RCE Vulnerability Let Attackers Execute Remote Code With Elevated Privileges	https://cybersecuritynews.com/longwatch-rce-vulnerability/
K7 Antivirus Vulnerability Allows Attackers Gain SYSTEM-level Privileges	https://cybersecuritynews.com/k7-antivirus-vulnerability/

Patches / Updates / Fixes

Εδώ θα βρείτε τις πιο πρόσφατες διορθώσεις και ενημερώσεις ασφαλείας από προμηθευτές λογισμικού και hardware. Το περιεχόμενο αφορά συγκεκριμένα bugs ή exploits που έχουν ήδη δημοσιοποιηθεί, μαζί με οδηγίες για το πώς να εφαρμοστούν τα patches.

Σύντομη περιγραφή / Τίτλος	URL
Chrome 143 Patches High-Severity Vulnerabilities	https://www.securityweek.com/chrome-143-patches-high-severity-vulnerabilities/
Akamai Patches HTTP Request Smuggling Vulnerability in Edge Servers	https://cybersecuritynews.com/akamai-http-request-smuggling-vulnerability/

Potential threats / Threat intelligence

Η συγκεκριμένη ενότητα ασχολείται με νέες απειλές, εξελιγμένα malware και τεχνικές επιθέσεων που έχουν εντοπιστεί σε πραγματικές συνθήκες. Περιλαμβάνονται αναφορές σε εργαλεία που χρησιμοποιούν οι επιτιθέμενοι, αλλά και δείκτες (IoCs) που μπορούν να χρησιμοποιηθούν στην άμυνα.

Σύντομη περιγραφή / Τίτλος	URL
Beware of Solana Phishing Attacks That Let Hackers Initiate Unauthorized Account Transfer	https://cybersecuritynews.com/beware-of-solana-phishing-attacks/
New SVG Clickjacking Attack Let Attackers Create Interactive Clickjacking Attacks	https://cybersecuritynews.com/svg-clickjacking-attack/
New Phishing Attack Mimic as Income Tax Department of India Delivers AsyncRAT	https://cybersecuritynews.com/new-phishing-attack-mimic-as-income-tax-department/

Guides / Tools

Παρουσιάζονται τεχνικοί οδηγοί και εργαλεία που μπορούν να βοηθήσουν στην παρακολούθηση, ανάλυση ή ενίσχυση της ασφάλειας συστημάτων. Είτε πρόκειται για open source projects είτε για νέες τεχνικές, η ενότητα αυτή λειτουργεί ως πόρος για πρακτικές λύσεις στην καθημερινή δουλειά των επαγγελματιών ασφάλειας.

Σύντομη περιγραφή / Τίτλος	URL
Top Tools for Enterprise Security Monitoring	https://cybersecuritynews.com/enterprise-security-monitoring-tools/
10 Best Vulnerability Management Tools In 2025	https://cybersecuritynews.com/vulnerability-management-tools/
Splunk Releases Guide to Detect Remote Employment Fraud Within Your Organization	https://cybersecuritynews.com/detect-remote-employment-fraud/
Top 15 Best Security Incident Response Tools In 2025	https://cybersecuritynews.com/incident-response-tools/
10 Best API Protection Tools in 2025	https://cybersecuritynews.com/best-api-protection-tools/
ThreatBook Launches Best-of-Breed Advanced Threat Intelligence Solution	https://cybersecuritynews.com/threatbook-advanced-threat-intelligence-solution/

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.

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/