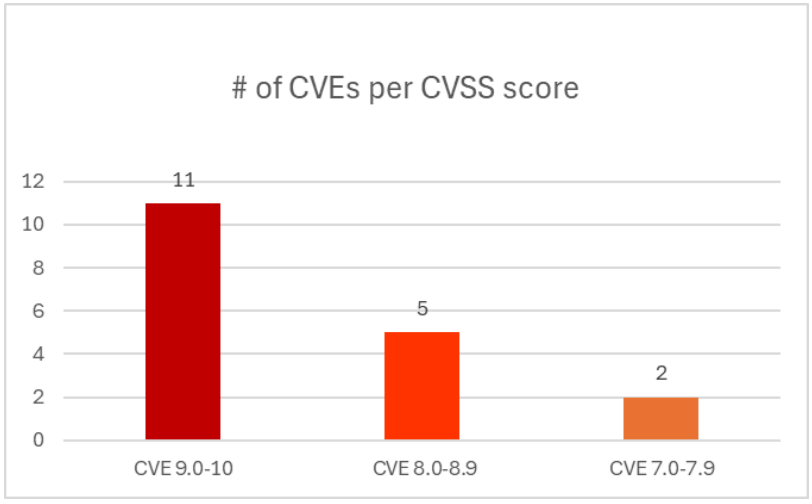
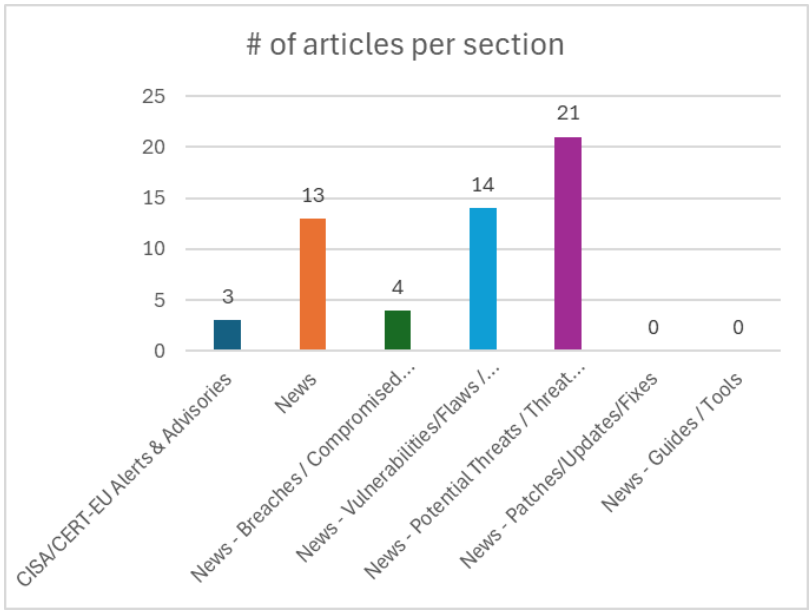
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 30/09/2025 - 03/10/2025





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-2025-34217	10,0	Vasion Print (formerly PrinterLogic)	Use of Hard-coded Cryptographic Key	Vasion Print (formerly PrinterLogic) Virtual Appliance Host and Application (VA/SaaS deployments)	https://help.printerlogic.com/saas/Print/Security/Security-Bulletins.htm https://help.printerlogic.com/va/Print/Security/Security-Bulletins.htm https://pierrekim.github.io/blog/2025-04-08-vasion-printerlogic-83-vulnerabilities.html#va-undocumented-hardcoded-ssh-key https://www.vulncheck.com/advisories/vasion-print-printerlogic-incorrect-encryption-algorithms-used-to-store-passwords
https://nvd.nist.gov/vuln/detail/CVE-2025-8120	10,0	PAD CMS	Unrestricted Upload of File with Dangerous Type	PAD CMS	https://cert.pl/posts/2025/09/CVE-2025-7063
https://nvd.nist.gov/vuln/detail/CVE-2025-10725	9,9	Red Hat Openshift AI Service	Incorrect Privilege Assignment	Red Hat Openshift AI Service	https://access.redhat.com/errata/RHSA-2025:16981 https://access.redhat.com/errata/RHSA-2025:16982 https://access.redhat.com/errata/RHSA-2025:16983 https://access.redhat.com/errata/RHSA-2025:16984 https://access.redhat.com/security/cve/CVE-2025-10725 https://bugzilla.redhat.com/show_bug.cgi?id=2396641
https://nvd.nist.gov/vuln/detail/CVE-2025-10659	9,8	MegaSys Telenium	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Telenium Online Web Application	https://support.portal.megasys.com/ https://www.cisa.gov/news-events/ics-advisories/icsa-25-273-01
https://nvd.nist.gov/vuln/detail/CVE-2025-61622	9,8	Python Pyfory	Deserialization of Untrusted Data	pyfory versions 0.12.0 through 0.12.2, or the legacy pyfury versions from 0.1.0 through 0.10.3	https://lists.apache.org/thread/vfn9hp9qt06db5yo1gmj3l114o3o2csd
https://nvd.nist.gov/vuln/detail/CVE-2025-34235	9,5	Vasion Print (formerly PrinterLogic) Virtual Appliance Host	Improper Certificate Validation	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to version 25.1.102 and Application prior to version 25.1.1413 (Windows client deployments)	https://help.printerlogic.com/saas/Print/Security/Security-Bulletins.htm https://help.printerlogic.com/va/Print/Security/Security-Bulletins.htm https://pierrekim.github.io/blog/2025-04-08-vasion-printerlogic-83-vulnerabilities.html#win-lpe-04 https://www.vulncheck.com/advisories/vasion-print-printerlogic-weak-ssl-tls-certificate-validation-rce

https://nvd.nist.gov/vuln/detail/CVE-2025-30247	9,3	Western Digital My Cloud	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	An OS command injection vulnerability in user interface in Western Digital My Cloud firmware prior to 5.31.108 on NAS platforms	https://www.westerndigital.com/support/product-security/wdc-25006-western-digital-my-cloud-os-5-firmware-5-31-108
https://nvd.nist.gov/vuln/detail/CVE-2025-59954	9,3	Knowage	Improper Control of Generation of Code ('Code Injection')	Knowage is an open source analytics and business intelligence suite. Versions 8.1.26 and below	https://github.com/KnowageLabs/Knowage-Server/commit/1bb60d42557724f7ed24c19df6c5017e169527ca https://github.com/KnowageLabs/Knowage-Server/security/advisories/GHSA-96cv-75hg-xrgq
https://nvd.nist.gov/vuln/detail/CVE-2025-61584	9,3	serverless-dns	Improper Neutralization of Special Elements used in a Command ('Command Injection')	serverless-dns is a RethinkDNS resolver that deploys to Cloudflare Workers, Deno Deploy, Fastly, and Fly.io. Versions through abd including 0.1.30	https://github.com/serverless-dns/serverless-dns/commit/c5537dd7f203c59f2b86d1e295c2371f3533946a https://github.com/serverless-dns/serverless-dns/security/advisories/GHSA-9g7x-737f-5xpc
https://nvd.nist.gov/vuln/detail/CVE-2024-58040	9,1	Crypt::RandomEncryption for Perl	Insufficient Entropy	Crypt::RandomEncryption for Perl version 0.01 uses insecure rand() function during encryption	https://metacpan.org/release/QWER/Crypt-RandomEncryption-0.01/source/lib/Crypt/RandomEncryption.pm#L33 https://perldoc.perl.org/functions/rand https://security.metacpan.org/docs/guides/random-data-for-security.html
https://nvd.nist.gov/vuln/detail/CVE-2025-7493	9,1	FreeIPA	Insufficient Granularity of Access Control	A privilege escalation flaw from host to domain administrator was found in FreeIPA. This vulnerability is similar to CVE-2025-4404, where it fails to validate the uniqueness of the krbCanonicalName	https://access.redhat.com/errata/RHSA-2025:17084 https://access.redhat.com/errata/RHSA-2025:17085 https://access.redhat.com/errata/RHSA-2025:17086 https://access.redhat.com/errata/RHSA-2025:17087 https://access.redhat.com/errata/RHSA-2025:17088 https://access.redhat.com/errata/RHSA-2025:17129 https://access.redhat.com/security/cve/CVE-2025-7493 https://bugzilla.redhat.com/show_bug.cgi?id=2389448
https://nvd.nist.gov/vuln/detail/CVE-2025-36245	8,8	IBM InfoSphere	mproper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	IBM InfoSphere 11.7.0.0 through 11.7.1.6 Information Server	https://www.ibm.com/support/pages/node/7246170
https://nvd.nist.gov/vuln/detail/CVE-2025-59684	8,8	DigiSign DigiSigner	Uncontrolled Search Path Element	DigiSign DigiSigner ONE 1.0.4.60	https://digisign.ro/products-services/signing-applications/ https://github.com/Henkel-CyberVM/CVEs/tree/main/CVE-2025-59684
https://nvd.nist.gov/vuln/detail/CVE-2025-7779	8,8	Acronis	Improper Privilege Management	Acronis True Image (macOS) before build 42389, Acronis True Image for SanDisk (macOS) before build 42198, Acronis True Image for Western	https://security-advisory.acronis.com/advisories/SEC-8193

				Digital (macOS) before build 42197	
https://nvd.nist.gov/vuln/detail/CVE-2025-23293	8,7	NVIDIA	Missing Authentication for Critical Function	NVIDIA Delegated Licensing Service for all appliance platforms	https://nvd.nist.gov/vuln/detail/CVE-2025-23293 https://nvidia.custhelp.com/app/answers/detail/a_id/5705 https://www.cve.org/CVERecord?id=CVE-2025-23293
https://nvd.nist.gov/vuln/detail/CVE-2025-10847	8,4	Broadcom Nimsoft DX Unified Infrastructure Management	Improper Access Control		https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36180
https://nvd.nist.gov/vuln/detail/CVE-2025-24525	7,5	Keysight Ixia Vision	Use of Hard-coded Cryptographic Key		https://support.ixiacom.com/ https://support.ixiacom.com/support-overview/product-support/downloads-updates https://www.cisa.gov/news-events/ics-advisories/icsa-25-063-02 https://www.keysight.com/us/en/contact.html
https://nvd.nist.gov/vuln/detail/CVE-2025-45376	7,5	Dell	Improper Handling of Insufficient Permissions or Privileges	Dell Repository Manager (DRM), versions 3.4.7 and 3.4.8	https://www.dell.com/support/kbdoc/en-us/000375461/dsa-2025-373-security-update-for-dell-repository-manager-vulnerability

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 Ten Industrial Control Systems Advisories	▪ ICSA-25-273-01 MegaSys Enterprises Telenium Online Web Application ▪ ICSA-25-273-02 Festo SBRD-Q/SBOC-Q/SBOI-Q ▪ ICSA-25-273-03 Festo CPX-CEC-C1 and CPX-CMXX ▪ ICSA-25-273-04 Festo Controller CECC-S,-LK,-D Family Firmware ▪ ICSA-25-273-05 OpenPLC_V3 ▪ ICSA-25-273-06 National Instruments Circuit Design Suite ▪ ICSA-25-273-07 LG Innotek Camera Multiple Models ▪ ICSA-25-063-02 Keysight Ixia Vision Product Family (Update A) ▪ ICSA-22-298-02 HEIDENHAIN Controller TNC (Update A) ▪ ICSA-25-226-26 Rockwell Automation FLEX 5000 I/O (Update A)	https://www.cisa.gov/news-events/alerts/2025/09/30/cisa-releases-ten-industrial-control-systems-advisories
CISA Adds Five Known Exploited Vulnerabilities to Catalog	▪ CVE-2014-6278 GNU Bash OS Command Injection Vulnerability ▪ CVE-2015-7755 Juniper ScreenOS Improper Authentication Vulnerability ▪ CVE-2017-1000353 Jenkins Remote Code Execution Vulnerability	https://www.cisa.gov/news-events/alerts/2025/10/02/cisa-adds-five-known-exploited-vulnerabilities-catalog

	▪ CVE-2025-4008 Smartbed-ded Meteobridge Command Injec-tion Vulnerability ▪ CVE-2025-21043 Samsung Mobile Devices Out-of-Bounds Write Vulnerability	
CISA Releases Two Industrial Control Systems Advisories	▪ ICSA-25-275-01 Raise3D Pro2 Series 3D Printers ▪ ICSA-25-275-02 Hitachi Energy MSM Product	https://www.cisa.gov/news-events/alerts/2025/10/02/cisa-releases-two-industrial-control-systems-advisories

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
Red Hat Confirms Data Breach After Hackers Claim to Steal 570GB of Private GitHub Repositories	https://cybersecuritynews.com/red-hat-confirms-data-breach/
Microsoft Defender for Endpoint Bug Triggers Numerous False BIOS Alerts	https://cybersecuritynews.com/microsoft-defender-endpoint-bug/
Microsoft to Launch New Secure Default Settings for Exchange and Teams APIs	https://cybersecuritynews.com/secure-default-exchange-and-teams/
New Obex Tool Blocks EDR Dynamic Libraries From Loading at Runtime	https://cybersecuritynews.com/obex-blocks-edr-dynamic-libraries/
PoC exploit Released for VMware Workstation guest-to-host escape Vulnerability	https://cybersecuritynews.com/vmware-workstation-vulnerability/
Microsoft Outlook for Windows Bug Leads to Crash While Opening Email	https://cybersecuritynews.com/microsoft-outlook-windows-bug/
New Google Drive Desktop Feature adds AI-powered Ransomware Detection to Pre-vent Cyberattacks	https://cybersecuritynews.com/google-drive-ransomware-detection/
New Battering RAM Attack Bypasses Latest Defenses on Intel and AMD Cloud Pro-cessors	https://cybersecuritynews.com/battering-ram-attack/
Microsoft Investigating Widespread Outlook.com Outage Preventing Users from Ac-cessing Mailbox	https://cybersecuritynews.com/widespread-outlook-com-outage/
How SOC Teams Detect Can Detect Cyber Threats Quickly Using Threat Intelligence Feeds	https://cybersecuritynews.com/soc-cyber-threat-detection/
Hackers Actively Scanning to Exploit Palo Alto Networks PAN-OS Global Protect Vul-nerability	https://cybersecuritynews.com/pan-os-global-protect-vulnerability/
Linux 6.17 Released With Fix for use-after-free Vulnerabilities	https://cybersecuritynews.com/linux-6-17-released/
Fake Postmark MCP Server Silently Stole Thousands of Emails With a Single Line of Malicious Code	https://cybersecuritynews.com/fake-postmark-mcp-server/

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
Red Hat Data Breach – Threat Actors Claim Breach of 28K Private GitHub Repositories	https://cybersecuritynews.com/red-hat-data-breach/
Allianz Life Data Breach Exposes Personal Records of 1.5 Million Users	https://cybersecuritynews.com/allianz-life-data-breach-report/
WestJet Confirms Data Breach – Customers Personal Information Exposed	https://cybersecuritynews.com/westjet-data-breach/
Beer Brewing Giant Asahi Halts Production Following Cyberattack	https://cybersecuritynews.com/asahi-cyberattack/

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
Chrome Security Update Patches 21 Vulnerabilities that Allow Attackers to Execute Arbitrary Code	https://cybersecuritynews.com/chrome-security-updates/
Multiple Splunk Enterprise Vulnerabilities Let Attackers Execute Unauthorized JavaScript code	https://cybersecuritynews.com/splunk-enterprise-vulnerabilities/
AI-Powered FunkLocker Ransomware Leverages Windows utilities to Disable Defenses	https://cybersecuritynews.com/ai-powered-funklocker-ransomware/
Red Hat Openshift AI Service Vulnerability Lets Attackers Take Full Control of Cloud Infrastructure	https://cybersecuritynews.com/red-hat-openshift-ai-service-vulnerability/
48+ Cisco Firewalls Vulnerable to Actively Exploited 0-Day Vulnerability in the Wild	https://cybersecuritynews.com/cisco-firewalls-vulnerability-exploited/
Windows 11 25H2 Released for General Availability – Know Issues and Mitigations	https://cybersecuritynews.com/windows-11-25h2/
CISA Warns of Linux Sudo Vulnerability Actively Exploited in Attacks	https://cybersecuritynews.com/cisa-linux-sudo-vulnerability/
Google Gemini Vulnerabilities Let Attackers Exfiltrate Users' Saved Data and Location	https://cybersecuritynews.com/google-gemini-vulnerabilities/
Tesla's Telematics Control Unit Vulnerability Let Attackers Gain Code Execution as Root	https://cybersecuritynews.com/teslas-telematics-control-unit-vulnerability/
VMware Tools and Aria 0-Day Vulnerability Exploited to Escalate Privileges and Execute Code as Root	https://cybersecuritynews.com/vmware-tools-0-day-vulnerability/
VMware Tools and Aria Operations Vulnerabilities Let Attackers Escalate Privileges to Root	https://cybersecuritynews.com/vmware-tools-and-aria-operations-vulnerabilities/

Critical Western Digital My Cloud NAS Vulnerability Allows Remote Code Execution	https://cybersecuritynews.com/western-digital-my-cloud-devices-vulnerability/
Apple Font Parser Vulnerability Enables Malicious Fonts to Corrupt Process Memory	https://cybersecuritynews.com/apple-font-parser-vulnerability/
VMware vCenter and NSX Vulnerabilities Let Attackers Enumerate Valid Usernames	https://cybersecuritynews.com/vmware-vcenter-and-nsx-vulnerabilities/

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

Potential threats / Threat intelligence

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

Σύντομη περιγραφή / Τίτλος	URL
Ukraine Warns of Weaponized XLL Files Delivers CABINETRAT Malware Via Zip Files	https://cybersecuritynews.com/cabinetrat-malware-via-zip-files/
Threat Actors Leveraging Senior Travel Scams to Deliver Datzbro Malware	https://cybersecuritynews.com/threat-actors-deliver-datzbro-malware/
Malicious PyPI Package Mimics as SOCKS5 Proxy Tool Attacking Windows Platforms	https://cybersecuritynews.com/malicious-pypi-package-mimics-as-socks5-proxy-tool/
New FlipSwitch Hooking Technique Bypasses Linux Kernel Defenses	https://cybersecuritynews.com/new-flipswitch-hooking-technique/
New DNS Malware Detour Dog Delivers Strela Stealer Using DNS TXT Records	https://cybersecuritynews.com/new-dns-malware-detour-dog/
Hackers Abuse EV Certificates to Sign Completely Undetectable DMG Malware	https://cybersecuritynews.com/hackers-abuse-ev-certificates/
Google Releases Guide to Harden Security Strategy and Detection Capabilities Against UNC6040	https://cybersecuritynews.com/google-releases-guide-against-unc6040/
CISA Warns of Cisco IOS and IOS XE SNMP Vulnerabilities Exploited in Attacks	https://cybersecuritynews.com/cisco-ios-and-ios-xe-snmp-vulnerabilities/
MatrixPDF Attacks Gmail Users Bypassing Email Filters and Fetch Malicious Payload	https://cybersecuritynews.com/matrixpdf-attacks-gmail-users-bypassing-email-filters/
Patchwork APT Using PowerShell Commands to Create Scheduled Task and Downloads Final Payload	https://cybersecuritynews.com/patchwork-apt-using-powershell-commands/
New Chinese Nexus APT Hackers Attacking Organizations to Deliver NET-STAR Malware Suite	https://cybersecuritynews.com/new-chinese-nexus-apt-hackers-attacking-organizations/
Hackers Posing as Google Careers Recruiter to Steal Gmail Login Details	https://cybersecuritynews.com/hackers-posing-as-google-careers-recruiter/
Hackers Exploit Cellular Router's API to Send Malicious SMS Messages With Weaponized Links	https://cybersecuritynews.com/hackers-exploit-cellular-routers-api/

New Android Banking Trojan Uses Hidden VNC to Gain Complete Remote Control Over Device	https://cybersecuritynews.com/new-android-banking-trojan-uses-hidden-vnc/
OpenSSL Vulnerabilities Let Attackers Execute Malicious Code and Recover Private Key Remotely	https://cybersecuritynews.com/openssl-vulnerabilities/
Beware! Threat Actors Distributing Malicious AI Tools as Chrome Extensions	https://cybersecuritynews.com/threat-actors-distributing-malicious-ai-tools/
CISA Warns of Libraesva ESG Command Injection Vulnerability Actively Exploited in Attacks	https://cybersecuritynews.com/cisa-warns-of-libraesva-esg-command-injection-vulnerability/
Threat Actors Hijacking MS-SQL Server to Deploy XiebroC2 Framework	https://cybersecuritynews.com/threat-actors-hijacking-ms-sql-server/
APT35 Hackers Attacking Government, Military Organizations to Steal Login Credentials	https://cybersecuritynews.com/apt35-hackers-attacking-government-military-organizations/
Threat Actors Allegedly Listed Veeam RCE Exploit for Sale on Dark Web	https://cybersecuritynews.com/threat-actors-allegedly-listed-veeam-rce-exploit/
Lunar Spider Infected Windows Machine in Single Click to Harvest Login Credentials	https://cybersecuritynews.com/lunar-spider-infected-windows-machine/

Guides / Tools

Παρουσιάζονται τεχνικοί οδηγοί και εργαλεία που μπορούν να βοηθήσουν στην παρακολούθηση, ανάλυση ή ενίσχυση της ασφάλειας συστη-μάτων. Είτε πρόκειται για open source projects είτε για νέες τεχνικές, η ενότητα αυτή λειτουργεί ως πόρος για πρακτικές λύσεις στην καθημε-ρινή δουλειά των επαγ-γελματιών ασφάλειας.

Σύντομη περιγραφή / Τίτλος	URL

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/