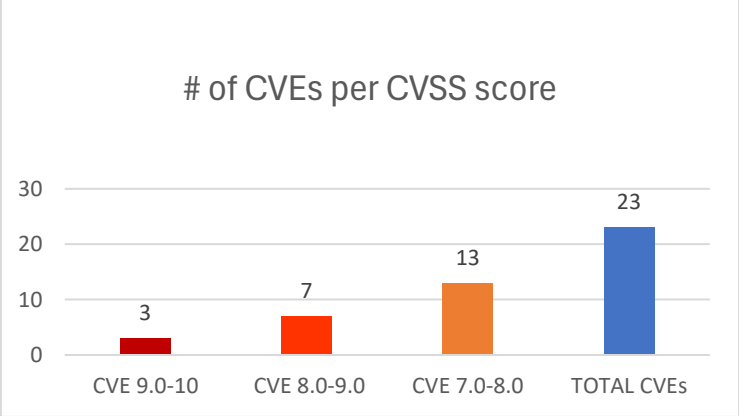
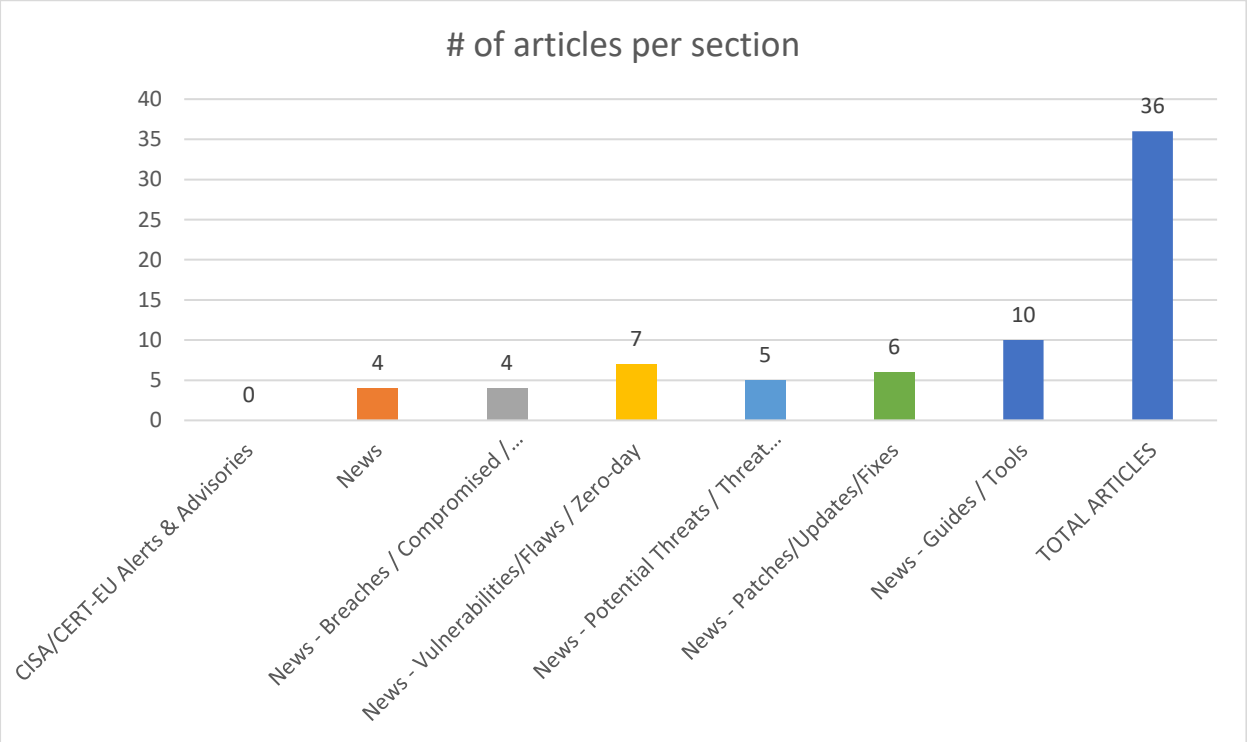
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 21/03/2026 - 24/03/2026





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-2026-4585	9,8	Tiandy Easy7 Integrated Management Platform	Improper Neutralization of Special Elements used in a Command ('Command Injection')	up to 7.17.0	https://my.feishu.cn/docx/WkHjd3oa-jolw5exHk9ecUHaFnKd?from=from_copylink VulDB https://vuldb.com/?ctiid.352422 VulDB https://vuldb.com/?id.352422 VulDB https://vuldb.com/?submit.775457
https://nvd.nist.gov/vuln/detail/CVE-2026-4753	9,1	slajerek RetroDebugger	Out-of-bounds Read	before v0.64.72	https://github.com/slajerek/RetroDebugger/pull/97
https://nvd.nist.gov/vuln/detail/CVE-2026-4750	9,1	fabiangreffrath woof	Out-of-bounds Read	before woof_15.3.0	https://github.com/fabiangreffrath/woof/pull/2521
https://nvd.nist.gov/vuln/detail/CVE-2026-4680	8,8	FedCM in Google Chrome	Use After Free	prior to 146.0.7680.165	https://chromereleases.google-blog.com/2026/03/stable-channel-update-for-desktop_23.html Chrome https://issues.chromium.org/issues/491869946
https://nvd.nist.gov/vuln/detail/CVE-2026-4678	8,8	WebGPU in Google Chrome	Use After Free	prior to 146.0.7680.165	https://chromereleases.google-blog.com/2026/03/stable-channel-update-for-desktop_23.html Chrome https://issues.chromium.org/issues/491164019
https://nvd.nist.gov/vuln/detail/CVE-2026-4677	8,8	WebAudio in Google Chrome	Out-of-bounds Read	prior to 146.0.7680.165	https://chromereleases.google-blog.com/2026/03/stable-channel-update-for-desktop_23.html Chrome https://issues.chromium.org/issues/490533968

https://nvd.nist.gov/vuln/detail/CVE-2026-4639	8,8	Vitals ESP developed by Galaxy Software Services	Incorrect Authorization		https://www.twcert.org.tw/en/cp-139-10795-25784-2.html TWCERT/CC https://www.twcert.org.tw/tw/cp-132-10794-704a2-1.html
https://nvd.nist.gov/vuln/detail/CVE-2026-4553	8,8	Tenda	Stack-based Buffer Overflow	F453 1.0.0.3	https://github.com/Li-tengzheng/vul_db/blob/main/F453/vul_88/README.md VulDB https://vuldb.com/?ctiid.352380 VulDB https://vuldb.com/?id.352380 VulDB https://vuldb.com/?submit.774931 VulDB https://www.tenda.com.cn/
https://nvd.nist.gov/vuln/detail/CVE-2026-4566	8,8	Belkin	Improper Restriction of Operations within the Bounds of a Memory Buffer	F9K1122 1.00.33	https://github.com/Li-tengzheng/vul_db/blob/main/Belkin/vul_151/README.md VulDB https://github.com/Li-tengzheng/vul_db/blob/main/Belkin/vul_151/README.md#proof-of-concept-poc VulDB https://vuldb.com/?ctiid.352403 VulDB https://vuldb.com/?id.352403 VulDB https://vuldb.com/?submit.775132
https://nvd.nist.gov/vuln/detail/CVE-2026-4558	8,8	Linksys	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	MR9600 2.0.6.206937	https://github.com/utmost3/cve/issues/1 VulDB https://vuldb.com/?ctiid.352385 VulDB https://vuldb.com/?id.352385 VulDB https://vuldb.com/?submit.775036 VulDB https://www.linksys.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-4756	7,8	MolotovCherry Android-ImageMagick7	Out-of-bounds Write	before 7.1.2-11	https://github.com/MolotovCherry/Android-ImageMagick7/pull/194
https://nvd.nist.gov/vuln/d	7,5	github.com/antchfx/xpath	Loop with Unreachable Exit Condition ('Infinite Loop')		https://access.redhat.com/security/cve/CVE-2026-4645 Red Hat, Inc. https://bugzilla.redhat.com/show_bug.cgi?id=2450

etail/CVE-2026-4645					214 Red Hat, Inc. https://github.com/antchfx/xpath/commit/afd4762cc342af56345a3fb4002a59281fcab494 Red Hat, Inc. https://github.com/antchfx/xpath/issues/121 Red Hat, Inc. https://github.com/golang/vulndb/issues/4526
https://nvd.nist.gov/vuln/detail/CVE-2026-4662	7,5	The JetEngine plugin for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	all versions up to, and including, 3.8.6.1	https://crocoblock.com/changelog/?plugin=jet-engine Wordfence https://plugins.trac.wordpress.org/browser/jet-engine/tags/3.8.6.1/includes/components/listings/ajax-handlers.php#L251 Wordfence https://plugins.trac.wordpress.org/browser/jet-engine/tags/3.8.6.1/includes/components/query-builder/listings/query.php#L125 Wordfence https://plugins.trac.wordpress.org/browser/jet-engine/tags/3.8.6.1/includes/components/query-builder/queries/sql.php#L1038 Wordfence https://plugins.trac.wordpress.org/browser/jet-engine/tags/3.8.6.1/includes/components/query-builder/queries/sql.php#L962 Wordfence https://www.wordfence.com/threat-intel/vulnerabilities/id/f10cf49b-1b78-43c1-b0d1-c1dbb74d5696?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2026-4598	7,5	jsrsasign	Loop with Unreachable Exit Condition ('Infinite Loop')	before 11.1.1	https://gist.github.com/Kr0emer/a1bf5cd4547cc630d2dcc5e761de8264 Snyk Exploit_Mitigation_Third Party Advisory https://github.com/kjur/jsrsasign/commit/ca5b027240287a1e71fe63019fc4400332594323 Snyk Patch https://github.com/kjur/jsrsasign/pull/648 Snyk Issue Tracking

					https://security.snyk.io/vuln/SNYK-JS-JSRSASIGN-15370938
https://nvd.nist.gov/vuln/detail/CVE-2026-4613	7,3	SourceCodester E-Commerce Site	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	1.0	https://github.com/WHOAMI-xiaoyu/CVE/blob/main/CVE_4.md VulDB https://vuldb.com/?ctiid.352477 VulDB https://vuldb.com/?id.352477 VulDB https://vuldb.com/?submit.775689 VulDB https://www.sourcecodester.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-4617	7,3	SourceCodester Patients Waiting Area Queue Management System	Improper Authorization	1.0	https://gist.github.com/HxH404/0ab53ccba44456b5400a5908414f5ab1 VulDB https://vuldb.com/?ctiid.352481 VulDB https://vuldb.com/?id.352481 VulDB https://vuldb.com/?submit.775747 VulDB https://www.sourcecodester.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-4623	7,3	DefaultFuction Jeson-Customer-Relationship-Management-System	Server-Side Request Forgery (SSRF)	up to 1b4679c4d06b90d31dd521c2b000bfdec5a36e00	https://github.com/DefaultFuction/Jeson-Customer-Relationship-Management-System/ VulDB https://github.com/DefaultFuction/Jeson-Customer-Relationship-Management-System/commit/f76e7123fe093b8675f88ec8f71725b0dd186310 VulDB https://github.com/DefaultFuction/Jeson-Customer-Relationship-Management-System/issues/2 VulDB https://github.com/DefaultFuction/Jeson-Customer-Relationship-Management-System/issues/2#issue-4045330588 VulDB https://github.com/DefaultFuction/Jeson-Customer-Relationship-Management-System/issues/2#issuecomment-4023480586 VulDB https://vuldb.com/?ctiid.352482 VulDB https://vuldb.com/?id.352482 VulDB https://vuldb.com/?submit.775760

https://nvd.nist.gov/vuln/detail/CVE-2026-4632	7,3	Online Enrollment System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/chuxina7-aiguo/CVE1/issues/1 VulDB https://itsourcecode.com/ VulDB https://vuldb.com/?ctiid.352499 VulDB https://vuldb.com/?id.352499 VulDB https://vuldb.com/?submit.775856
https://nvd.nist.gov/vuln/detail/CVE-2026-4612	7,3	Free Hotel Reservation System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://github.com/bybinyu/Vulnerability-Practice/issues/2 VulDB https://itsourcecode.com/ VulDB https://vuldb.com/?ctiid.352476 VulDB https://vuldb.com/?id.352476 VulDB https://vuldb.com/?submit.775645
https://nvd.nist.gov/vuln/detail/CVE-2026-4580	7,3	Simple Laundry System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1.0	https://code-projects.org/ VulDB https://github.com/anon387tdug/anon388/issues/2 VulDB https://vuldb.com/?ctiid.352417 VulDB https://vuldb.com/?id.352417 VulDB https://vuldb.com/?submit.775210
https://nvd.nist.gov/vuln/detail/CVE-2026-4562	7,3	MacCMS	Missing Authentication for Critical Function	202.510.004.052	https://github.com/HuajiHD/CVE/issues/9 VulDB https://vuldb.com/?ctiid.352399 VulDB https://vuldb.com/?id.352399 VulDB https://vuldb.com/?submit.775039
https://nvd.nist.gov/vuln/detail/CVE-2026-4627	7,2	D-Link DIR-825 and DIR-825R 1.0.5/4.5.1	Improper Neutralization of Special Elements used in a Command ('Command Injection')		https://vuldb.com/?ctiid.352495 VulDB https://vuldb.com/?id.352495 VulDB https://vuldb.com/?submit.775794 VulDB https://www.dlink.com/
https://nvd.nist.gov/vuln/detail/CVE-2026-4611	7,2	TOTOLINK	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	X6000R 9.4.0cu.1360_B20241207/9.4	https://vuldb.com/?ctiid.352475 VulDB https://vuldb.com/?id.352475 VulDB https://vuldb.com/?submit.775642 VulDB https://www.totolink.net/

			.0cu.1498_B20250826	

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
-		-

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 Orders US Government to Patch Maximum Severity Cisco Flaw	https://www.infosecurity-magazine.com/news/cisa-orders-us-government-patch/
Operation Alice Takes Down 370,000+ Dark Web Sites	https://www.infosecurity-magazine.com/news/operation-alice-370000-dark-web/
FBI, CISA Warn Russian Hackers Are Targeting High-Value Individuals Through Signal	https://cybersecuritynews.com/fbi-cisa-warn-russian-hackers/
Libyan Oil Refinery Hit in Long-Running Espionage Campaign Using AsyncRAT	https://cybersecuritynews.com/libyan-oil-refinery-hit-in-long-running-espionage/

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
511,000+ End-of-Life Microsoft IIS Instances Exposed Online, Secure Now!	https://cybersecuritynews.com/iis-end-of-life-instances-exposed/
Mazda Data Breach Exposing Employee and Partner Records Via System Vulnerability	https://cybersecuritynews.com/mazda-data-breach/

Crunchyroll Data Breach — Threat Actor Claims Exfiltration of 100 GB of User Data	https://cybersecuritynews.com/crunchyroll-data-breach/
AstraZeneca Data Breach – LAPSUS$ Group Allegedly Claims Access to Internal Data	https://cybersecuritynews.com/astrazeneca-data-breach/

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
Hackers Exploit CVE-2025-32975 (CVSS 10.0) to Hijack Unpatched Quest KACE SMA Systems	https://thehackernews.com/2026/03/hackers-exploit-cve-2025-32975-cvss-100.html
CISA Flags Apple, Craft CMS, Laravel Bugs in KEV, Orders Patching by April 3, 2026	https://thehackernews.com/2026/03/cisa-flags-apple-craft-cms-laravel-bugs.html
Critical Quest KACE Vulnerability Potentially Exploited in Attacks	https://www.securityweek.com/critical-quest-kace-vulnerability-potentially-exploited-in-attacks/
Oracle Issues Urgent Security Update for Critical RCE Flaw in Identity Manager and Web Services Manager	https://cybersecuritynews.com/oracle-urgent-security-update/
Critical QNAP QVR Pro Vulnerability Let Remote Attackers Gain Access to the System	https://cybersecuritynews.com/qnap-qvr-pro-vulnerability/
CISA Warns of Craft CMS Code Injection Vulnerability Exploited in Attacks	https://cybersecuritynews.com/cms-code-injection-vulnerability-exploited/
CISA Warns of Apple Vulnerabilities Linked to DarkSword iOS Exploit Chain Exploited in Attacks	https://cybersecuritynews.com/apple-vulnerabilities-darksword-ios-exploit/

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
Oracle Patches Critical CVE-2026-21992 Enabling Unauthenticated RCE in Identity Manager	https://thehackernews.com/2026/03/oracle-patches-critical-cve-2026-21992.html
QNAP Patches Four Vulnerabilities Exploited at Pwn2Own	https://www.securityweek.com/qnap-patches-four-vulnerabilities-exploited-at-pwn2own/
Oracle Releases Emergency Patch for Critical Identity Manager Vulnerability	https://www.securityweek.com/oracle-releases-emergency-patch-for-critical-identity-manager-vulnerability/
Chrome Security Update Fixes 26 Vulnerabilities Allowing Remote Code Execution	https://cybersecuritynews.com/chrome-security-update-patches-26-vulnerabilities/
Microsoft Emergency Out-of-Band Update for Windows 11 to Fix Microsoft Account Sign-In Failure	https://cybersecuritynews.com/windows-11-account-sign-in-failure/
Citrix Urges Patching Critical NetScaler Flaw Allowing Unauthenticated Data Leaks	https://thehackernews.com/2026/03/citrix-urges-patching-critical.html

Potential threats / Threat intelligence

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

Σύντομη περιγραφή / Τίτλος	URL
MacOS Stealer MioLab Adds ClickFix Delivery, Wallet Theft and Team API Tools	https://cybersecuritynews.com/macos-stealer-miolab/
Oblivion RAT Turns Fake Play Store Updates Into a Full-Service Android Spyware Operation	https://cybersecuritynews.com/oblivion-rat-turns-fake-play-store-updates/
New CanisterWorm Steals npm Tokens and Spreads Through Compromised Pub-lisher Accounts	https://cybersecuritynews.com/new-canisterworm-steals-npm-tokens/
Tycoon2FA Phishing Service Resumes Activity Post-Takedown	https://www.infosecurity-magazine.com/news/tycoon2fa-phishing-service-resumes/
Trivy Supply Chain Attack Expands With New Compromised Docker Images	https://www.infosecurity-magazine.com/news/trivy-supply-chain-attack-expands/

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 επαγ-γελματιών ασφάλειας.

Σύντομη περιγραφή / Τίτλος	URL
Top Tools for Enterprise Security Monitoring	**https://cybersecuritynews.com/enterprise-security-monitoring-tools/**
Splunk Releases Guide to Detect Remote Employment Fraud Within Your Organization	https://cybersecuritynews.com/detect-remote-employment-fraud/
ThreatBook Launches Best-of-Breed Advanced Threat Intelligence Solution	https://cybersecuritynews.com/threatbook-advanced-threat-intelligence-solution/
CISA Releases Best Security Practices Guide for Hardening Microsoft Exchange Server	https://cybersecuritynews.com/microsoft-exchange-server-hardening-guide/
Top 10 Best Exposure Management Tools In 2026	https://cybersecuritynews.com/best-exposure-management-tools/
NETREAPER Offensive Security Toolkit That Wraps 70+ Penetration Testing Tools	https://cybersecuritynews.com/netreaper-offensive-security-toolkit/
GitLab Security Best Practices Cheat Sheet	https://thehackernews.uk/gitlab-security-tips
False Negatives Are a New SOC Headache. Here's the Fast Way to Fix It	https://cybersecuritynews.com/false-negatives-are-a-new-soc-headache-heres-the-fast-way-to-fix-it/
PentAGI – Automated AI-Powered Penetration Testing Tool that Integrates 20+ Security Tools	https://cybersecuritynews.com/pentagi-penetration-testing-tool/
The CISO Executive Toolkit (Free Download)	https://thehackernews.uk/wiz-ciso-bundle

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/