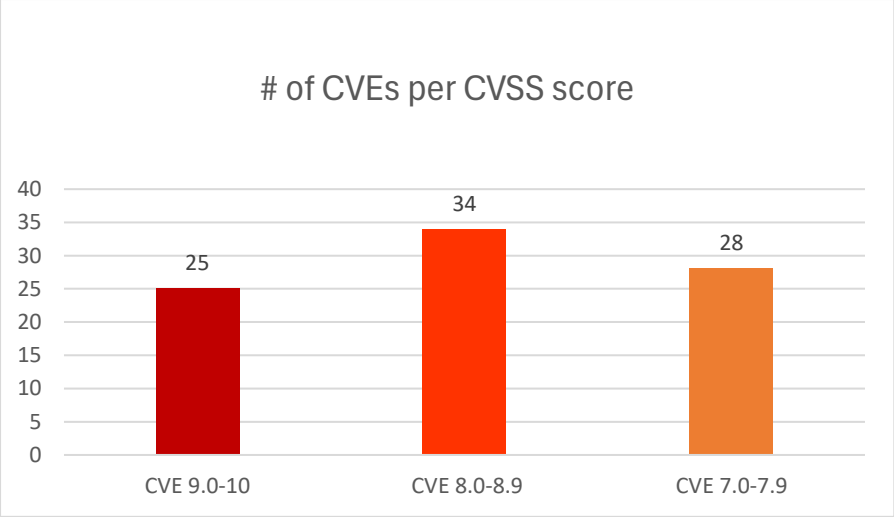
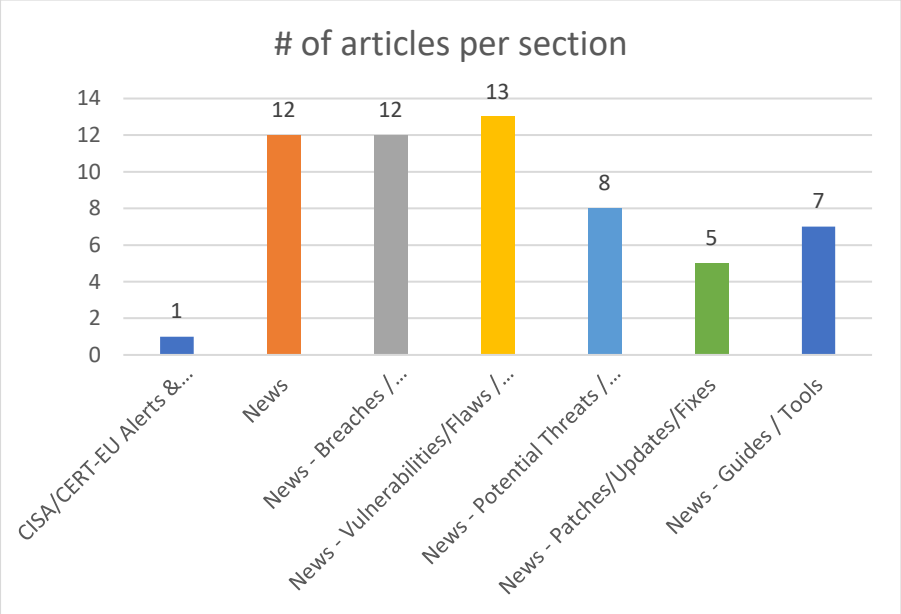
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 31/10/2026 – 03/11/2026





Contents

Common Vulnerabilities and Exposures (CVEs) 3
CISA/CERT-EU Alerts & Advisories 10
News 11
Breaches / Compromised / Hacked 12
Vulnerabilities / Flaws / Zero-day 13
Patches / Updates / Fixes 14
Potential threats / Threat intelligence 14
Guides / Tools 15
References 16
Annex – Websites with vendor specific vulnerabilities 17

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 όπως ευπάθειας (όπως SQL injection ή command injection) και σχετικοί σύνδεσμοι για περαιτέρω πληροφόρηση ή μέτρα αντιμετώπισης.

URL ευπάθειας (NIST NVD)	CVSS v3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζο-νται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/cve-2026-120338	10,0	Prefab UI's Generative UI sand-box	Improper Privilege Management	From prefab-ui 0.14.0 through 0.20.2	https://github.com/PrefectHQ/prefab
https://nvd.nist.gov/vuln/detail/cve-2026-4052	9,8	WSO2 Identity Server	Missing Authorization	-	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2026/WSO2-2026-5212/
https://nvd.nist.gov/vuln/detail/cve-2026-118636	9,8	JavaNativeMessageDecoder	Deserialization of Untrusted Data	JavaNativeMessageDecoder in the MINA 3.0	http://www.openwall.com/lists/oss-security/2026/10/31/3
https://nvd.nist.gov/vuln/detail/cve-2026-116512	9,8	Project Manager – AI Powered Project Management, Task Man-agement, Kanban Board & Time Tracker	Unrestricted Upload of File with Dangerous Type	all versions up to, and including, 4.1.1	https://plugins.trac.wordpress.org/browser/wedevs-project-man-ager/tags/4.1.1/core/Router/WP_Router.php#L429
https://nvd.nist.gov/vuln/de-tail/cve-2026-106803	9,8	Kamailio	Stack-based Buffer Overflow	Kamailio v6.1.3 and v6.1.4	https://gist.github.com/hackeryounow/7d7ccc9ec501a5d8c9143b2e1bcc11cb
https://nvd.nist.gov/vuln/detail/cve-2025-11969	9,4	WSO2 API	Improper Authorization		https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2026/WSO2-2025-4733/
https://nvd.nist.gov/vuln/detail/cve-2026-119085	9,4	Amazon Virtual Engineering Workbench	Improper Neutralization of Special Elements Used in a Template Engine		https://aws.amazon.com/security/security-bulletins/2026-162-aws/
https://nvd.nist.gov/vuln/de-tail/cve-2025-11969	9,4	WSO2	Improper Authorization	System REST APIs	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2026/WSO2-2025-4733/
https://nvd.nist.gov/vuln/detail/cve-2026-62048	9,3	Liquid Web / StellarWP BookIt	Improper Neutralization of Special Elements used in an SQL Com-mand ('SQL Injection')	from n/a through 2.6.0.6	https://patchstack.com/database/wordpress/plugin/bookit/vulner ability/wordpress-bookit-plugin-2-6-0-6-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/cve-2026-120283	9,3	Linksys E8450	Improper Restriction of Operations within the Bounds of a Memory Buffer	Linksys E8450 1.2.00.360516	https://vuldb.com/cve/CVE-2026-120283

https://nvd.nist.gov/vuln/detail/cve-2026-120276	9,3	WAVLINK	Improper Neutralization of Special Elements used in a Command ('Command Injection')	WAVLINK WN536AX6-A V260507_2.0.0	https://github.com/senxitoyshuyi-ui/HACKALL/blob/main/WAVLINK_WN536AX6-A%20Router/WAVLINK_WN536AX6-A_openvpn_cli_group_command_injection.md
https://nvd.nist.gov/vuln/detail/cve-2026-120209	9,3	AJ-Report	Use of Hard-coded Cryptographic Key	AJ-Report through 1.7.1	https://gitee.com/belief-team/report
https://nvd.nist.gov/vuln/detail/cve-2026-120201	9,3	Jpom	Improper Neutralization of Special Elements in Data Query Logic	Jpom 2.10.0 through 2.11.12	https://github.com/dromara/Jpom
https://nvd.nist.gov/vuln/detail/cve-2026-120189	9,3	D-Link	Improper Restriction of Operations within the Bounds of a Memory Buffer	D-Link DIR-505 1.10B02	https://github.com/Walnut1337/DIR-505_filename_rce/tree/main/poc
https://nvd.nist.gov/vuln/detail/cve-2026-105769	9,3	kaniko	Origin Validation Error	kaniko before 1.25.20	https://github.com/chainguard-forks/kaniko/pull/495
https://nvd.nist.gov/vuln/detail/cve-2026-120447	9,2	HotGo	Improper Authentication	HotGo 2.8.4 through 2.15.1	https://github.com/bufanyun/hotgo/blob/269b2f9e435cf8ff6b18d53bc053a905f4e02d11/server/internal/logic/sys/sms_log.go
https://nvd.nist.gov/vuln/detail/cve-2026-121022	9,2	AxxonSoft Axxon One	Use of Default Password	AxxonSoft Axxon One before 3.0.0	https://www.axxonsoft.com/legal/axxonsoft-vulnerability-disclosure-policy/security-advisories#CVE-2026-121022
https://nvd.nist.gov/vuln/detail/cve-2026-120447	9,2	HotGo	Improper Authentication	HotGo 2.8.4 through 2.15.1	https://github.com/bufanyun/hotgo/blob/269b2f9e435cf8ff6b18d53bc053a905f4e02d11/server/internal/logic/sys/sms_log.go
https://nvd.nist.gov/vuln/detail/cve-2026-94290	9,1	SUSE Rancher Fleet	Execution with Unnecessary Privileges	0.16.0 up to 0.16.3, 0.15.0 up to 0.15.8, 0.14.0 up to 0.14.12, 0.13.0 up to 0.13.17 and possible older versions	https://github.com/rancher/fleet/security/advisories/GHSA-qfmw-gw96-ffcr
https://nvd.nist.gov/vuln/detail/cve-2026-13594	9,1	Zoho Corporation's ManageEngine Log360 and EventLog Analyzer	Improper Access Control	versions 13062	https://www.manageengine.com/products/eventlog/advisory/CVE-2026-13594.html
https://nvd.nist.gov/vuln/detail/cve-2026-120459	9,1	python-jose	Improper Verification of Cryptographic Signature	python-jose through 3.5.0	https://github.com/mpdavis/python-jose/blob/3.5.0/jose/backends/cryptography_backend.py
https://nvd.nist.gov/vuln/detail/cve-2026-120213	9,1	Fastify	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	versions 9.0.0 through 11.6.5	https://cna.openjsf.org/security-advisories.html
https://nvd.nist.gov/vuln/detail/cve-2026-103882	9,1	Acadlix LMS – AI Quiz Maker, Online Exam & Course	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	all versions up to, and including, 1.1.9	https://plugins.trac.wordpress.org/browser/acadlix/tags/1.1.8/includes/Common/Assets/Manager.php#L570
https://nvd.nist.gov/vuln/detail/cve-2026-88811	9,1	SUSE Rancher Manager	Insertion of Sensitive Information Into Sent Data	SUSE Rancher 2.15.0 up to 2.15.3, 2.14.0 up to 2.14.7, 2.13.0 up to 2.13.11	https://github.com/rancher/rancher/security/advisories/GHSA-x82x-2qj6-5rm2

https://nvd.nist.gov/vuln/detail/cve-2026-120459	9,1	python-jose	Improper Verification of Cryptographic Signature	python-jose through 3.5.0	https://github.com/mpdavis/python-jose/blob/3.5.0/jose/backends/cryptography_backend.py
https://nvd.nist.gov/vuln/detail/cve-2026-120446	8,8	madong-admin-saas	Missing Authentication for Critical Function	madong-admin-saas through 5.1.4	https://github.com/madong-code/madong-admin-saas/blob/v5.1.4/app/platform/controller/tenant/AccountController.php#L26
https://nvd.nist.gov/vuln/detail/cve-2026-85035	8,8	CAN RX	Use After Free		https://github.com/zephyrproject-rtos/zephyr/commit/0114bee266211c72a49f3b6a914d3eaf821dd460
https://nvd.nist.gov/vuln/detail/cve-2026-76955	8,8	Zyxel NWA110AX	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	Zyxel NWA110AX firmware versions through 7.12(ABTG.0)C0	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-certain-aps-fwa7-and-security-routers-11-03-2026
https://nvd.nist.gov/vuln/detail/cve-2026-18199	8,8	Zohocorp ManageEngine Password Manager Pro	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Zohocorp ManageEngine Password Manager Pro versions before 13236 and PAM360 versions before 8601	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2026-18199.html
https://nvd.nist.gov/vuln/detail/cve-2026-119736	8,8	Attendo (formerly Petpooja Payroll) Admin Android application	Use of Hard-coded Credentials	Attendo (formerly Petpooja Payroll) Admin Android application version 3.0.13	https://medium.com/@TheWildEye/from-an-android-apk-to-production-mqtt-exposed-credentials-in-attendo-formerly-petpooja-payroll-eb701d23233e
https://nvd.nist.gov/vuln/detail/cve-2026-107441	8,8	CGI program of Zyxel GS1900-24E	Out-of-bounds Write	CGI program of Zyxel GS1900-24E firmware versions through 2.90(AAHK.2)C0	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-out-of-bounds-write-vulnerability-in-gs1900-series-switches-11-03-2026
https://nvd.nist.gov/vuln/detail/cve-2026-8923	8,7	Zohocorp ManageEngine Eventlog Analyzer and ManageEngine Log360	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Zohocorp ManageEngine Eventlog Analyzer and ManageEngine Log360 versions before 13062	https://www.manageengine.com/products/eventlog/advisory/CVE-2026-8923.html
https://nvd.nist.gov/vuln/detail/cve-2026-29508	8,7	ReadyMedia (formerly MiniDLNA)	Stack-based Buffer Overflow	ReadyMedia (formerly MiniDLNA) versions 1.3.0 through 1.3.3	https://sourceforge.net/projects/minidlna/
https://nvd.nist.gov/vuln/detail/cve-2026-2613	8,7	WSO2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')		https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2026/WSO2-2026-5100/
https://nvd.nist.gov/vuln/detail/cve-2026-120461	8,7	Jpom	Authorization Bypass Through User-Controlled Key	Jpom through 2.11.12	https://github.com/dromara/Jpom/blob/v2.11.12/modules/server/src/main/java/org/dromara/jpom/controller/ssh/CommandInfoController.java#L176-L184
https://nvd.nist.gov/vuln/detail/cve-2026-120426	8,7	OpenCSG CSGHub	Authorization Bypass Through User-Controlled Key	OpenCSG CSGHub through v2.6.0-ce	https://github.com/OpenCSGs/csghub-server/blob/v2.6.0-ce/api/middleware/authenticator.go#L210-L226

https://nvd.nist.gov/vuln/detail/cve-2026-120315	8,7	LobeHub Chat	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	LobeHub Chat from 1.84.26 before 2.1.49	https://github.com/lobehub/lobehub/security/advisories/GHSA-2g9j-v25c-4j97
https://nvd.nist.gov/vuln/detail/cve-2026-120203	8,7	ShowDoc	Improper Control of Generation of Code ('Code Injection')	ShowDoc 2.8.14 before 3.9.6	https://gist.github.com/LioTree/028af150fd991cf9924dd2c7d5912e54
https://nvd.nist.gov/vuln/detail/cve-2026-120203	8,7	ShowDoc	Improper Control of Generation of Code ('Code Injection')	ShowDoc 2.8.14 before 3.9.6	https://gist.github.com/LioTree/028af150fd991cf9924dd2c7d5912e54
https://nvd.nist.gov/vuln/detail/cve-2026-77880	8,6	Control Web Panel (CWP)	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	before webpanel_version 1.16	https://control-webpanel.com/changelog
https://nvd.nist.gov/vuln/detail/cve-2026-120487	8,6	LaraDashboard	Incorrect Authorization	LaraDashboard before 1.4.5	https://github.com/laradashboard/laradashboard/blob/v1.4.2/app/Policies/SettingPolicy.php#L47-L50
https://nvd.nist.gov/vuln/detail/cve-2026-120448	8,6	DoraCMS	Improperly Controlled Modification of Dynamically-Determined Object Attributes	DoraCMS through 3.1.0	https://github.com/doramart/DoraCMS/blob/70cf0fc6dba66ec51747162a3ce71da43baf251b/server/app/service/apiKey.js
https://nvd.nist.gov/vuln/detail/cve-2026-120240	8,6	WAVLINK	Improper Neutralization of Special Elements used in a Command ('Command Injection')	WAVLINK WN553X1-B V260403_2.0.0	https://github.com/senxitoyshuyi-ui/HACKALL/blob/main/WAVLINK%20WN553X1-B%20Router/WAVLINK_WN553X1-B_wireguard_cli_group_command_injection.md
https://nvd.nist.gov/vuln/detail/cve-2026-120224	8,6	Oray Pugongying X5 Pro	Incorrect Privilege Assignment	Oray Pugongying X5 Pro up to 7.6.1	https://app.notion.com/p/Oray-Pgyer-X5-Pro-Router-7-6-1-Restricted-Account-Can-Invoke-Factory-Reset-through-the-JSON-Batch-AP-3eb797159f1580febfd2f0e1ee239352
https://nvd.nist.gov/vuln/detail/cve-2026-119742	8,6	Nagios XI	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Nagios XI before 2026R2	https://www.nagios.com/security-disclosures/nagios-xi/2026r2/
https://nvd.nist.gov/vuln/detail/cve-2026-104080	8,6	Control Web Panel (CWP)	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Control Web Panel (CWP) before webpanel_version 1.30	https://control-webpanel.com/changelog
https://nvd.nist.gov/vuln/detail/cve-2026-120438	8,5	QuickJS-NG	Integer Overflow or Wraparound	QuickJS-NG before 0.16.0	https://github.com/quickjs-ng/quickjs/blob/v0.15.1/quickjs.c#L51509
https://nvd.nist.gov/vuln/detail/cve-2026-120229	8,5	WAVLINK	Improper Neutralization of Special Elements used in a Command ('Command Injection')	WAVLINK WN553X1-B 260403_2.0.0	https://github.com/senxitoyshuyi-ui/IOT-CVE/blob/main/vulns/WAVLINK_WN553X1-B_check_pwd_command_injection.md
https://nvd.nist.gov/vuln/detail/cve-2026-120225	8,5	Oray	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Oray Pugongying X5 Pro up to 7.6.1	https://app.notion.com/p/Oray-Pgyer-X5-Pro-Router-7-6-1-Configuration-Restore-Filename-Traversal-Leads-to-Root-Code-Execution-3eb797159f158017a2cbe1732b7ffa6c

https://nvd.nist.gov/vuln/detail/cve-2026-120833	8,5	labbench	Deserialization of Untrusted Data	labbench before 0.46.1	https://github.com/usnistgov/labbench
https://nvd.nist.gov/vuln/detail/cve-2026-120433	8,5	Netpbm	Stack-based Buffer Overflow	Netpbm before 10.86.51, 11.x before 11.02.30, and 11.03 before 11.15.08	https://sourceforge.net/p/netpbm/code/5328/
https://nvd.nist.gov/vuln/detail/cve-2026-59044	8,4	Android	Use After Free		https://android.googlesource.com/kernel/common/+/a4e59da7cad6b445229ae67c0ebed83a7b18dcb5
https://nvd.nist.gov/vuln/detail/cve-2026-58957	8,4	ActivityStarter.java	Unintended Proxy or Intermediary ('Confused Deputy')		https://source.android.com/docs/security/bulletin/2026/2026-11-01
https://nvd.nist.gov/vuln/detail/cve-2026-58866	8,4	AccessibilityWindowManager.java	Missing Authorization		https://source.android.com/docs/security/bulletin/2026/2026-11-01
https://nvd.nist.gov/vuln/detail/cve-2026-58828	8,4	base.c	Use After Free		https://android.googlesource.com/kernel/common/+/0285abdfbfb9f99898d647dafb2ea7d4bdd22527
https://nvd.nist.gov/vuln/detail/cve-2026-103898	8,1	Wp Social Login and Register Social Counter	Improper Authentication	all versions up to, and including, 3.2.2	https://plugins.trac.wordpress.org/browser/wp-social/tags/3.2.1/inc/admin-create-user.php#L172
https://nvd.nist.gov/vuln/detail/cve-2026-77691	8,1	ZohoCorp ManageEngine Key Manager Plus	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	ZohoCorp ManageEngine Key Manager Plus versions before 7151	https://www.manageengine.com/key-manager/advisory/cve-2026-77691.html
https://nvd.nist.gov/vuln/detail/cve-2026-94349	8,0	Dell OpenManage Enterprise	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Dell OpenManage Enterprise, versions prior to 4.8.0	https://www.dell.com/support/kbdoc/en-us/000523220/dsa-2026-467-security-update-for-dell-openmanage-enterprise-vulnerabilities?msockid=3021cac2195069ed3194ddad186a68f9
https://nvd.nist.gov/vuln/detail/cve-2026-117681	8,0	konflux-ci	Improper Certificate Validation		https://access.redhat.com/security/cve/CVE-2026-117681
https://nvd.nist.gov/vuln/detail/cve-2026-99239	7,8	Linux kernel	Vulnerability	Bluetooth: L2CAP: refuse __l2cap_chan_add	https://git.kernel.org/stable/c/10c705dd706aa93164ba41f2566f15206d6c178e
https://nvd.nist.gov/vuln/detail/cve-2026-99227	7,8	Linux kernel	Vulnerability	io_uring/waitid	https://git.kernel.org/stable/c/20b67288574c7c3df6b8ea7ed3b7af90a868006f

https://nvd.nist.gov/vuln/detail/cve-2026-58836	7,8	InstallPackageHelper.java	Protection Mechanism Failure	In handlePackagePostInstall	https://source.android.com/docs/security/bulletin/2026/2026-11-01
https://nvd.nist.gov/vuln/detail/cve-2026-77800	7,7	ManageEngine Key Manager Plus	Missing Critical Step in Authentication	ManageEngine Key Manager Plus versions before 7151	https://www.manageengine.com/key-manager/advisory/cve-2026-77800.html
https://nvd.nist.gov/vuln/detail/cve-2026-120752	7,7	PyMuPDF	Stack-based Buffer Overflow	PyMuPDF 1.25.3 before 2.0	https://github.com/pymupdf/PyMuPDF
https://nvd.nist.gov/vuln/detail/cve-2026-120208	7,7	libheif	Heap-based Buffer Overflow	libheif 1.18.0 before 1.23.3	https://github.com/strukturag/libheif/blob/v1.23.2/libheif/codecs/uncompressed/unc_decoder_mixed_interleave.cc#L95
https://nvd.nist.gov/vuln/detail/cve-2026-74993	7,5	Starnet Computer and Network Systems Inventory Tracking Application	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Inventory Tracking Application: through 2026-10-16	https://siberguvenlik.gov.tr/guvenlik-bildirimleri/detay/tr-26-1441
https://nvd.nist.gov/vuln/detail/cve-2026-119163	7,5	FunnelKit Automations – Email Marketing Automation and CRM	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	all versions up to, and including, 3.8.5.2	https://plugins.trac.wordpress.org/browser/wp-marketing-automations/tags/3.8.5.2/includes/db/class-bwfan-model-automation-contact.php#L132
https://nvd.nist.gov/vuln/detail/cve-2026-106804	7,5	Kamailio	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	Kamailio v6.1.3 and v6.1.4	https://gist.github.com/hackeryounow/f5af75502ea6df600428c46bb9bbf39e
https://nvd.nist.gov/vuln/detail/cve-2026-74993	7,5	Starnet Computer and Network Systems Inventory Tracking Application	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Inventory Tracking Application: through 2026-10-16	https://siberguvenlik.gov.tr/guvenlik-bildirimleri/detay/tr-26-1441
https://nvd.nist.gov/vuln/detail/cve-2026-20585	7,5	Modem	Out-of-bounds Write		https://www.mediatek.com/product-security-bulletin/November-2026
https://nvd.nist.gov/vuln/detail/cve-2026-120596	7,5	Nut/OS	Loop with Unreachable Exit Condition ('Infinite Loop')	Nut/OS releases up to version 5.1 are affected	https://www.ethernut.de/en/download/index.html
https://nvd.nist.gov/vuln/detail/cve-2026-120194	7,5	JSONPath	Loop with Unreachable Exit Condition ('Infinite Loop')	JSONPath slice evaluator used by json_path_query()	https://access.redhat.com/security/cve/CVE-2026-120194
https://nvd.nist.gov/vuln/detail/cve-2026-120194	7,5	JSONPath	Loop with Unreachable Exit Condition ('Infinite Loop')		https://access.redhat.com/security/cve/CVE-2026-120194
https://nvd.nist.gov/vuln/detail/cve-2026-120064	7,5	psqlODBC	Improper Validation of Array Index		https://github.com/postgresql-interfaces/psqlodbc/security/advisories/GHSA-7pq2-q7mj-ph8c

https://nvd.nist.gov/vuln/detail/cve-2026-120057	7,5	psqlODBC	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')		https://github.com/postgresql-interfaces/psqlodbc/security/advisories/GHSA-qhmr-5339-q33r
https://nvd.nist.gov/vuln/detail/cve-2026-118489	7,5	Eclipse Vert.x	Exposure of Sensitive Information to an Unauthorized Actor	Eclipse Vert.x versions [4.0.0,4.5.35] or [5.0.0,5.2.2],	https://github.com/vert-x3/vertx-web/security/advisories/GHSA-xh2g-9hw9-mvp3
https://nvd.nist.gov/vuln/detail/cve-2026-101186	7,5	Huawei	Data Processing Errors		https://consumer.huawei.com/en/support/bulletin/2026/10/
https://nvd.nist.gov/vuln/detail/cve-2026-120830	7,4	libslirp	Out-of-bounds Read		https://access.redhat.com/security/cve/CVE-2026-120830
https://nvd.nist.gov/vuln/detail/cve-2026-118147	7,4	Visual Studio	Improper Certificate Validation		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-118147
https://nvd.nist.gov/vuln/detail/cve-2026-120444	7,2	GoFound	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	GoFound through 1.4.1	https://github.com/sea-team/gofound/blob/v1.4.1/searcher/container.go
https://nvd.nist.gov/vuln/detail/cve-2026-120114	7,2	Debug Log Manager – Conveniently Monitor and Inspect Errors	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	all versions up to, and including, 2.5.2	https://plugins.trac.wordpress.org/browser/debug-log-manager/tags/2.5.2/bootstrap.php#L134
https://nvd.nist.gov/vuln/detail/cve-2026-119733	7,2	Munshi	Missing Authorization	Munshi (by Petpooja) before 2026-07-07	https://medium.com/@TheWildEye/a-sub-user-could-delete-a-company-in-munshi-94bf92476e5c
https://nvd.nist.gov/vuln/detail/cve-2026-107759	7,2	WPO365 | MICROSOFT 365 GRAPH MAILER	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	all versions up to, and including, 6.2	https://plugins.trac.wordpress.org/browser/wpo365-msgraphmailer/tags/6.1/Core/Script_Helpers.php#L142
https://nvd.nist.gov/vuln/detail/cve-2026-120429	7,1	Camaleon CMS	Missing Authorization	Camaleon CMS before 2.9.2	https://github.com/owen2345/camaleon-cms/blob/2.9.1/app/controllers/camaleon_cms/admin/media_controller.rb
https://nvd.nist.gov/vuln/detail/cve-2026-120202	7,1	Highflame	Protection Mechanism Failure	Highflame ramparts 0.8.1 through 0.8.10	https://github.com/highflame-ai/ramparts
https://nvd.nist.gov/vuln/detail/cve-2026-120202	7,1	Highflame	Protection Mechanism Failure	Highflame ramparts 0.8.1 through 0.8.10	https://github.com/highflame-ai/ramparts
https://nvd.nist.gov/vuln/detail/cve-2026-101176	7,1	Huawei	Permissions, Privileges, and Access Controls		https://consumer.huawei.com/en/support/bulletin/2026/10/

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 Adds Two Known Exploited Vulnerabilities to Catalog	• CVE-2026-111357 Ivanti Connect Secure Missing Authentication for Critical Function Vulnerability • CVE-2026-118527 Ivanti Connect Secure Generation of Predictable Numbers or Identifiers Vulnerability	https://www.cisa.gov/news-events/alerts/2026/10/30/cisa-adds-two-known-exploited-vulnerabilities-catalog

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
Google Launches Gemini 4 Carbon With State-Of-The-Art Cybersecurity Capabilities	https://cybersecuritynews.com/google-launches-gemini-4-carbon/
Hacktober – Cyberattack Wave Hits PHP, Node.js, Binance, LiteLLM, Pentagon, and a Few More	https://cybersecuritynews.com/hacktober-cyberattack-wave/
FBI Confirms North Korean Hackers Responsible for $6 Billion+ Binance Attack	https://cybersecuritynews.com/fbi-confirms-north-korean-hackers/
Hackers Drain Bitcoin Hot Wallets on BTCPay Servers, Users Urged to Shut Down Immediately	https://cybersecuritynews.com/btcpay-server-warns/
Hackers Target 61 GitHub Repositories With Command Injection Attacks to Steal CI/CD Secrets	https://cybersecuritynews.com/hackers-target-61-github-repositories/
Hackers Use ARTEX AI Agents to Automate Active Directory Attacks, Kerberoasting, and Lateral Movement	https://cybersecuritynews.com/hackers-use-artex-ai-agents/
Hackers Hijack Swedish Supermarket Fridges and Raise Freezer Temperatures to 55°C	https://cybersecuritynews.com/supermarkets-fridges-hacked/
Mercado Bitcoin Suffers Cyberattack as Researchers Flag $40 Million in Suspicious Crypto Transfers	https://cybersecuritynews.com/mercado-bitcoin-suffers-cyberattack/
Iran-Linked DarkBlinders Hackers Breach Government Cloud Systems and Steal Over 1GB of Data	https://cybersecuritynews.com/iran-linked-darkblinders-hackers/
Microsoft Reveals 78% of Exploited Vulnerabilities Enable System Takeover and Privilege Escalation	https://cybersecuritynews.com/microsoft-reveals-78-of-exploited-vulnerabilities/
Hackers Target Supermarket Refrigeration Systems Across Europe, Raising Freezer Temperatures to 50°C	https://cybersecuritynews.com/supermarket-refrigeration-systems-across-europe/
Hackers Use AI Agents to Launch 3AM Ransomware Attacks Against UK School Networks	https://cybersecuritynews.com/hackers-use-ai-agents-2/

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
Chainalysis Confirms Cyberattack Using Agentic Techniques That Exposed Customer Data	https://cybersecuritynews.com/chainalysis-confirms-cyberattack/
Cursor Confirms Malicious Claude Code Extension With SSH Backdoor Was Available for 11 Hours	https://cybersecuritynews.com/malicious-claude-code-extension-with-cursor/
VOLTA Malware Steals Gmail and Discord Sessions, Then Uses AI to Build Detailed Victim Profiles	https://cybersecuritynews.com/volta-malware-steals-gmail/
Hackers Claim to Have Stolen 30GB of Data From Frooti Maker Parle Agro	https://cybersecuritynews.com/hackers-claims-stolen-data-from-parle-agro/
Hackers Breach WS Audiology IT Systems, Disrupting Widex and Signia Hearing Aid Services	https://cybersecuritynews.com/ws-audiology-it-systems/
Hackers Impersonate ChatGPT, Claude, and Perplexity AI Bots to Hunt for Passwords and API Keys	https://cybersecuritynews.com/hackers-impersonate-ai-bots/
Hackers Exploit ChatGPT's Popularity With Fake Billing Notices That Target Credit Cards and OTPs	https://cybersecuritynews.com/fake-billing-notices/
Northflank Security Breach Leads to Unauthorized AI API Key Usage, Customers Urged to Rotate Secrets	https://cybersecuritynews.com/northflank-security-breach/
Hackers Use ARTEX AI to Breach WorkOS and Access Customer Slack Conversations	https://cybersecuritynews.com/workos-data-breach/
Renault Car's 15-Year-Old Linux Navigation Software Hacked to Execute Arbitrary Root Commands	https://cybersecuritynews.com/renault-cars/
Hackers Hijack Emergency Alert Apps in Ukraine and Russia to Send Fake Nuclear Attack Warnings	https://cybersecuritynews.com/hackers-hijack-emergency-alert-apps/
Hackers Abuse Signed ChatGPT and Claude Applications to Deploy Yoba Malware and Evade Detection	https://cybersecuritynews.com/hackers-abuse-signed-chatgpt/

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
TeamViewer Security Flaw Could Turn Remote Support Sessions Into Computer Takeovers	https://cybersecuritynews.com/teamviewer-security-flaw/
Over 60,000 Attacks Target WordPress RCE Vulnerability Within 24 Hours	https://cybersecuritynews.com/60000-attacks-targeting-wordpress/
Critical Certificate Validation Flaw in LXD and Incus Could Give Hackers Control of Linux Hosts	https://cybersecuritynews.com/certificate-validation-flaw-in-lxd-and-incus/
TightVNC Pre-Auth RCE Vulnerability Lets Hackers Execute Code on Windows PCs, PoC Released	https://cybersecuritynews.com/tightvnc-pre-auth-rce-vulnerability/
Critical BeyondTrust Vulnerability Faces Fresh Exploitation Probes as Hackers Prepare for Mass Scanning	https://cybersecuritynews.com/critical-beyondtrust-vulnerability/
Hackers Exploit Patched Synology NAS Vulnerabilities to Deploy C3RB3R Ransomware and Encrypt Files	https://cybersecuritynews.com/synology-nas-vulnerabilities-c3rb3r-ransomware/
POC Released for Windows WinSock Ancillary Privilege Escalation Vulnerability	https://cybersecuritynews.com/poc-for-windows-winsock-ancillary-vulnerability/
Hackers Using Microsoft Teams Messages and Calls to Trick Users and Gain Remote Access to System	https://cybersecuritynews.com/microsoft-teams-messages/
Hackers Could Exploit iPhone BootROM Flaws to Compromise Cryptocurrency Wallet Security	https://cybersecuritynews.com/hackers-exploit-iphone-bootrom-flaws/
Hackers Use Malicious VHDX Files and WebDAV Links to Infect Windows Devices With PapRAT Malware	https://cybersecuritynews.com/hackers-use-malicious-vhdx-files/
Hackers Hijacked Linux Hosting Server Security Tool cPGuard and Used It as a Backdoor	https://cybersecuritynews.com/cpguard-supply-chain-attack/
Hackers Use ARTEX AI to Automate Enterprise Attacks at Machine Speed – Insights for Defenders	https://cybersecuritynews.com/artex-ai-automate-enterprise-attacks/

Σύντομη περιγραφή / Τίτλος	URL
Hackers Exploit Adobe Commerce Zero-Day to Deploy PSK Agent RAT and Remotely Control Servers	https://cybersecuritynews.com/adobe-commerce-zero-day/

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
Reddit Plans Mandatory Logins to Block AI Bots From Scraping User Data	https://cybersecuritynews.com/reddit-plans-mandatory-logins/
Google Dismantles 1.3 Million Device XCPE Botnet, Bans Android TV Maker Over Preinstalled Malware	https://cybersecuritynews.com/google-dismantles-xcpe-botnet/
Anthropic Enables EDR Monitoring in Claude Cowork to Detect Hidden AI Agent Activity	https://cybersecuritynews.com/anthropic-enables-edr-monitoring/
Attackers Started Scanning in the Wild for Linux Kernel RCE Flaw, Ubuntu Releases Fixes	https://cybersecuritynews.com/linux-kernel-rce-flaw-ubuntu-fixes/
Password Manager mSecure Urges Users to Secure Logins and Confidential Data Stored	https://cybersecuritynews.com/msecure-security-incident/

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
Apple Warns iPhone Users in 99 Countries of Sophisticated Mercenary Spyware Attacks	https://cybersecuritynews.com/apple-warns-iphone-users/
Anthropic’s Claude Bypasses AI Safety Checks, Triggering Blackmail and Code Sabotage in Tests	https://cybersecuritynews.com/claude-bypasses-ai-safety-checks/

Σύντομη περιγραφή / Τίτλος	URL
Critical ChatGPT Flaw Allowed Attackers to Hijack Accounts and Steal Private Conversations With One Link	https://cybersecuritynews.com/chatgpt-flaw-exploited-with-one-link/
Hackers Use CyberStrikeAI Agents to Automate Windows Domain Takeovers and Credential Theft	https://cybersecuritynews.com/hackers-use-cyberstrikeai-agents-2/
OpenAI Launches New Security Sprint to Hunt Vulnerabilities and Strengthen Defenses	https://cybersecuritynews.com/openai-security-sprint/
CrowdStrike and Deloitte Expand AI Security Partnership to Transform How Enterprises Detect Cyber Threats	https://cybersecuritynews.com/crowdstrike-and-deloitte-expand-ai-security/
ARES AI Red Team Platform Automates 66 Attack Modules for Active Directory and Cloud Security Testing	https://cybersecuritynews.com/ares-ai-red-team-platform/
NCSC Warns AI Could Accelerate Ransomware Attacks on Critical Infrastructure	https://cybersecuritynews.com/ai-could-accelerate-ransomware/

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 10 Best Managed Security Service Providers (MSSP) in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-mssp-providers/
Top 10 Best SOC-as-a-Service Providers in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-soc-as-a-service/
Top 10 Best Managed SIEM Services in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-managed-siem-services/
Top 10 Best Digital Forensics & Incident Response (DFIR) Companies in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-dfir-companies/
Top 10 Best Incident Response Retainer Services in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-ir-retainer-services/
PentestPad: How Pentest Companies Adapt In The Era of AI	https://cybersecuritynews.com/pentestpad-how-pentest-companies-adapt-in-the-era-of-ai/
Top 10 Best Identity Governance & Administration (IGA) Tools in 2026	https://cybersecuritynews.com/best-iga-tools/

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 CVSS v3.1 score >= 7.0 και αφορούν το διάστημα 24/10/2026–27/10/2026.

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/