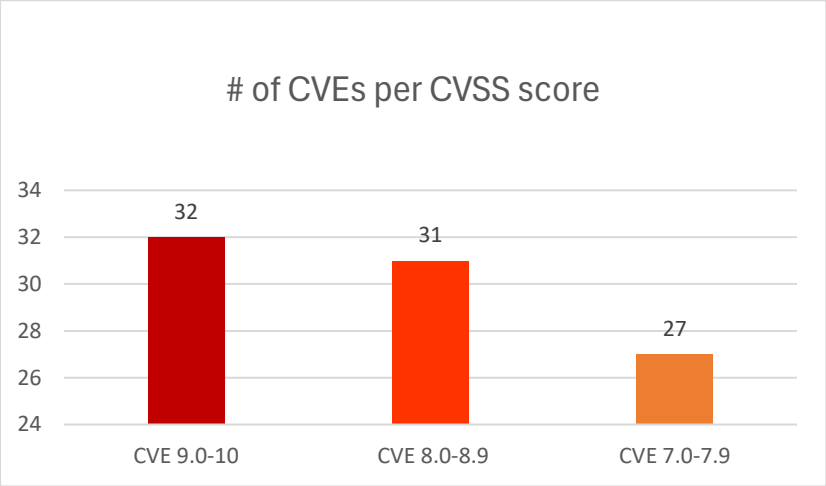
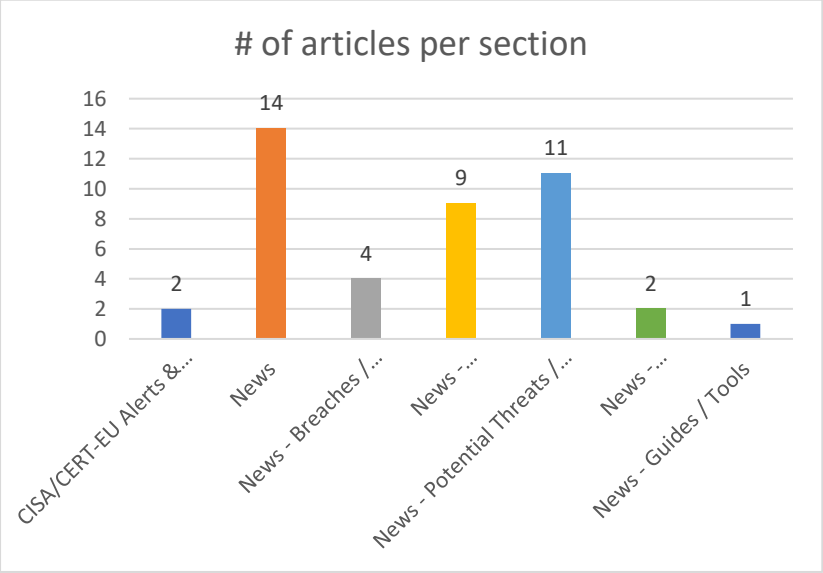


Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 07/11/2026 - 10/11/2026





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 επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώ-πισης
https://nvd.nist.gov/vuln/detail/cve-2026-89126	**10,0**	SAP Web Dispatcher	Heap-based Buffer Overflow	-	https://me.sap.com/notes/3778556
https://nvd.nist.gov/vuln/detail/cve-2026-89103	**10,0**	SAP Gateway	Incorrect Authorization	-	https://me.sap.com/notes/3798345
https://nvd.nist.gov/vuln/detail/cve-2026-76964	**10,0**	SAP NetWeaver Application Server ABAP	Improper Validation of Specified Type of Input	-	https://me.sap.com/notes/3778530
https://nvd.nist.gov/vuln/detail/cve-2026-120017	**10,0**	SAP NetWeaver AS ABAP and ABAP Platform	Improper Verification of Cryptographic Signature	-	https://me.sap.com/notes/3849308
https://nvd.nist.gov/vuln/detail/cve-2026-17158	**9,9**	IBM API Connect	Improper Authentication	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2	https://www.ibm.com/support/pages/node/7295635
https://nvd.nist.gov/vuln/detail/cve-2026-13312	**9,9**	Axis Communications AB	Improper Validation of Specified Type of Input	-	https://www.axis.com/dam/public/e4/2d/85/cve-2026-13312pdf-en-US-561251.pdf
https://nvd.nist.gov/vuln/detail/cve-2026-109795	**9,9**	SAP NetWeaver	Improper Control of Generation of Code ('Code Injection')	https://me.sap.com/notes/3834842	
https://nvd.nist.gov/vuln/detail/cve-2026-107331	**9,9**	IBM DataStage	Absolute Path Traversal	IBM DataStage on Cloud Pak for Data 5.4.0.0	https://www.ibm.com/support/pages/node/7294270
https://nvd.nist.gov/vuln/detail/cve-2026-16720	**9,8**	IBM API Connect	Improper Authentication	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2	https://www.ibm.com/support/pages/node/7295635
https://nvd.nist.gov/vuln/detail/cve-2026-6715	**9,8**	IBM Concert	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	IBM Concert 1.0 through 3.0.1.1	https://www.ibm.com/support/pages/node/7294607
https://nvd.nist.gov/vuln/detail/cve-2026-15266	**9,8**	IBM Concert	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	IBM Concert 1.0 through 3.0.1.1	https://www.ibm.com/support/pages/node/7294607

https://nvd.nist.gov/vuln/detail/cve-2026-125120	**9,8**	Mongoose	Improper Neutralization of Special Elements in Data Query Logic	Prior to 6.13.11, 7.8.12, 8.24.3, and 9.9.2	https://github.com/Automattic/mongoose/commit/7e912af3fac52cb0eea4cd71e24d65318916831a
https://nvd.nist.gov/vuln/detail/cve-2026-123807	**9,8**	Signal K Server	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	From 2.0.0 until 2.34.0 and from 1.0.0 until 1.5.3	https://github.com/SignalK/signalk-server/commit/83689f040d7e90280dddc643f44f3e4ce348fbb1G
https://nvd.nist.gov/vuln/detail/cve-2026-123270	**9,8**	Redpanda Connect	Missing Authentication for Critical Function	Redpanda Connect versions 4.39 to 4.110	https://github.com/pagvac/redpanda-connect-unauth-rce
https://nvd.nist.gov/vuln/detail/cve-2026-123614	**9,8**	imgproxy	Heap-based Buffer Overflow	imgproxy from 4.0.0 before 4.0.16	https://github.com/imgproxy/imgproxy/security/advisories/GHSA-hff9-5pqw-6w9f
https://nvd.nist.gov/vuln/detail/cve-2026-17297	**9,6**	IBM API Connect	URL Redirection to Untrusted Site ('Open Redirect')	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2	https://www.ibm.com/support/pages/node/7295635
https://nvd.nist.gov/vuln/detail/cve-2026-18838	**9,4**	IBM API Connect	Authentication Bypass by Spoofing	IBM API Connect 12.1.0.0 through 12.1.1.2	https://www.ibm.com/support/pages/node/7295635
https://nvd.nist.gov/vuln/detail/cve-2026-124490	**9,4**	OpenEMR	External Control of File Name or Path	OpenEMR before 8.3.0	https://github.com/openemr/openemr/security/advisories/GHSA-38jw-pwgq-9hpj
https://nvd.nist.gov/vuln/detail/cve-2026-124440	**9,4**	Kyverno	Unintended Proxy or Intermediary ('Confused Deputy')	Kyverno from 1.19.1 before 1.19.2	https://github.com/kyverno/kyverno/security/advisories/GHSA-39w8-hv5g-f73w
https://nvd.nist.gov/vuln/detail/cve-2026-119756	**9,3**	Tasmota	Buffer Access with Incorrect Length Value	Tasmota through 16.0.0	https://github.com/arendst/Tasmota/commit/e97e1e4f7e319a55caa1613aef1f25fc81bdb554
https://nvd.nist.gov/vuln/detail/cve-2026-114464	**9,3**	IBM Process Mining	Improper Access Control	IBM Process Mining 2.0.0 through 2.2.1	https://www.ibm.com/support/pages/node/7294875
https://nvd.nist.gov/vuln/detail/cve-2026-125384	**9,3**	INDOTALENT WHMS	Use of Default Credentials	INDOTALENT WHMS before 10.20261109	https://github.com/go2ismail/Asp.Net-Core-Inventory-Order-Management-System
https://nvd.nist.gov/vuln/detail/cve-2026-125370	**9,3**	Kubero	Use of Hard-coded Cryptographic Key	Kubero 3.0.0 through 3.1.1	https://github.com/kubero-dev/kubero
https://nvd.nist.gov/vuln/detail/cve-2026-125086	**9,3**	D-Link M60	Use of Hard-coded Password	D-Link M60 1.12.B01	https://github.com/XueDugu/dlink-m60-easymesh-mqtt-credential-evidence
https://nvd.nist.gov/vuln/detail/cve-2026-124079	**9,3**	rConfig	Deserialization of Untrusted Data	rConfig Core 8.0.0 before 8.2.19 and rConfig Pro before 8.4.1	https://github.com/rconfig/rconfig/releases/tag/core-8.2.19
https://nvd.nist.gov/vuln/detail/cve-2026-123966	**9,3**	Tenda AC19	Improper Restriction of Operations within the Bounds of a Memory Buffer	Tenda AC19 16.03.10.07	https://github.com/Tmzop/Tenda-AC19-saveParentControlInfo/blob/main/report.md

https://nvd.nist.gov/vuln/detail/cve-2026-114464	**9,3**	IBM Process Mining	Improper Access Control	IBM Process Mining 2.0.0 through 2.2.1	https://www.ibm.com/support/pages/node/7294875
https://nvd.nist.gov/vuln/detail/cve-2026-119756	**9,3**	Tasmota through 16.0.0	Buffer Access with Incorrect Length Value	Tasmota through 16.0.0	https://github.com/arendst/Tasmota/commit/e97e1e4f7e319a55caa1613aef1f25fc81bdb554
https://nvd.nist.gov/vuln/detail/cve-2026-124001	**9,2**	NASA JPL ION-DTN	Integer Overflow or Wraparound	NASA JPL ION-DTN 2.2.1b through 4.2.0	https://github.com/nasa-jpl/ION-DTN/releases/tag/ion-open-source-4.2.1-a.2
https://nvd.nist.gov/vuln/detail/cve-2026-17466	**9,1**	IBM Optim	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	IBM Optim 1.0.0, 1.1.0, and 1.2.0	https://www.ibm.com/support/pages/node/7289719
https://nvd.nist.gov/vuln/detail/cve-2026-101117	**9,1**	IBM WebSphere	Configuration	IBM WebSphere Extreme Scale 8.6.1.0 through 8.6.2.2	https://www.ibm.com/support/pages/node/7293764
https://nvd.nist.gov/vuln/detail/cve-2026-119506	**9,1**	DynamiApps	Incorrect Privilege Assignment	-	https://patchstack.com/database/wordpress/plugin/acf-frontend-form-element/vulnerability/wordpress-frontend-admin-by-dynamiapps-plugin-3-30-1-privilege-escalation-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/cve-2026-102643	**8,8**	AsyncSSH	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Prior to 2.24.1	https://github.com/ronf/asyncssh/commit/d4fc430d37b234cb35f1ba2cca834b2dbe1302cf
https://nvd.nist.gov/vuln/detail/cve-2026-9764	**8,8**	IBM Bob	Improper Control of Generation of Code ('Code Injection')	IBM Bob 1.0.4 through 2.0.1	https://www.ibm.com/support/pages/node/7291535
https://nvd.nist.gov/vuln/detail/cve-2026-95779	**8,8**	HPE Morpheus	Exposure of Sensitive Information to an Unauthorized Actor	-	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbvs05168en_us&docLocale=en_US
https://nvd.nist.gov/vuln/detail/cve-2026-95778	**8,8**	HPE Morpheus Software	-	-	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbvs05168en_us&docLocale=en_US
https://nvd.nist.gov/vuln/detail/cve-2026-66669	**8,8**	Suplugins Superb	Cross-Site Request Forgery (CSRF)	from n/a through 4.2.4	https://patchstack.com/database/wordpress/plugin/superb-blocks/vulnerability/wordpress-superb-addons-blocks-patterns-amp-theme-designer-plugin-4-2-4-cross-site-request-forgery-csrf-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/cve-2026-16283	**8,8**	Osbil Technology Ltd. OPanel	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	oPanel: before 1.20.66.	https://siberguvenlik.gov.tr/guvenlik-bildirimleri/detay/tr-26-1488
https://nvd.nist.gov/vuln/detail/cve-2026-12977	**8,8**	WildFly Core	Privilege Defined With Unsafe Actions	-	https://access.redhat.com/security/cve/CVE-2026-12977

https://nvd.nist.gov/vuln/detail/cve-2026-121843	**8,8**	Firefox for iOS	-	Firefox for iOS 160.0.	https://bugzilla.mozilla.org/show_bug.cgi?id=2083030
https://nvd.nist.gov/vuln/detail/cve-2026-121842	**8,8**	Firefox for iOS	-	Firefox for iOS 160.0.	https://bugzilla.mozilla.org/show_bug.cgi?id=2076233
https://nvd.nist.gov/vuln/detail/cve-2026-120839	**8,8**	WpTravelly	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusio	WpTravelly: from n/a through 2.3.8.	https://patchstack.com/database/wordpress/plugin/tour-booking-manager/vulnerability/wordpress-wptravelly-plugin-2-3-8-local-file-inclusion-vulnerability-2?_s_id=cve
https://nvd.nist.gov/vuln/detail/cve-2026-117545	**8,8**	IBM	Improper Authentication	IBM webMethods Integration Server 12.1	https://www.ibm.com/support/pages/node/7295298
https://nvd.nist.gov/vuln/detail/cve-2026-124553	**8,7**	BabelDOC	Allocation of Resources Without Limits or Throttling	BabelDOC from 0.3.61 before 0.7.0	https://github.com/funstory-ai/BabelDOC/blob/main/docs/release-notes/v0.7.0.md
https://nvd.nist.gov/vuln/detail/cve-2026-124441	**8,7**	Kyverno	Incorrect Authorization	Kyverno before 1.19.2	https://github.com/kyverno/kyverno/security/advisories/GHSA-vjfx-fp68-rh4v
https://nvd.nist.gov/vuln/detail/cve-2026-124439	**8,7**	Scriban	Uncontrolled Recursion	Scriban and Scriban.Signed before 7.5.3	https://github.com/scriban/scriban/security/advisories/GHSA-mvmw-9jxc-7pr2
https://nvd.nist.gov/vuln/detail/cve-2026-123576	**8,7**	Hickory DNS	Allocation of Resources Without Limits or Throttling	Hickory DNS 0.24.0 through 0.26.1	https://github.com/hickory-dns/hickory-dns/security/advisories/GHSA-2f4m-fq7w-mrgx
https://nvd.nist.gov/vuln/detail/cve-2026-123569	**8,7**	npm	Allocation of Resources Without Limits or Throttling	npm before 5.6.3	https://github.com/sveltejs/devalue/security/advisories/GHSA-33hq-fvwr-56pm
https://nvd.nist.gov/vuln/detail/cve-2026-123560	**8,7**	Zebra	Incomplete Cleanup	Zebra before 7.0.0	https://github.com/ZcashFoundation/zebra/security/advisories/GHSA-9hq5-pfgc-cx5h
https://nvd.nist.gov/vuln/detail/cve-2026-124429	**8,7**	Craft CMS	Incorrect Privilege Assignment	Craft CMS from 5.0.0 before 5.11.2	https://github.com/craftcms/cms/security/advisories/GHSA-v25r-wr32-jfg7
https://nvd.nist.gov/vuln/detail/cve-2026-119759	**8,6**	TrailBase	Authorization Bypass Through User-Controlled Key	TrailBase 0.28.2 before 0.35.10	https://github.com/trailbaseio/trailbase/releases#release-v0.35.10
https://nvd.nist.gov/vuln/detail/cve-2026-114713	**8,6**	UnrealIRCd	Improper Neutralization of Delimiters	UnrealIRCd 6.0.0 before 6.2.7.1	http://www.openwall.com/lists/oss-security/2026/11/08/1
https://nvd.nist.gov/vuln/detail/cve-2026-124585	**8,6**	Chengdu	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Chengdu Feiyuxing Technology VW2100 and VEC10GP 1.0 B-MB3W202-210825-r11775	https://github.com/C0KE/Feiyuxing-VROS-add_expmac-RCE/blob/main/poc_add_expmac.py

https://nvd.nist.gov/vuln/detail/cve-2026-17407	**8,5**	IBM API Connect	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2	https://www.ibm.com/support/pages/node/7295635
https://nvd.nist.gov/vuln/detail/cve-2026-116501	**8,4**	IBM Qiskit	Out-of-bounds Write	IBM Qiskit SDK 2.4.0 through 2.6.1	https://www.ibm.com/support/pages/node/7295237
https://nvd.nist.gov/vuln/detail/cve-2026-124492	**8,3**	SunEditor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	SunEditor before 3.4.0	https://github.com/JiHong88/suneditor/security/advisories/GHSA-5pp5-5qrp-vq56
https://nvd.nist.gov/vuln/detail/cve-2026-123601	**8,3**	Hickory DNS	Use of Incorrect Operator	Hickory DNS hickory-proto 0.25.0 through 0.26.0-alpha.1 and hickory-net 0.26.0-beta.1 before 0.26.2	https://github.com/hickory-dns/hickory-dns/security/advisories/GHSA-588m-chg6-8jqj
https://nvd.nist.gov/vuln/detail/cve-2026-119610	**8,2**	Gstreamer	Out-of-bounds Read	-	https://access.redhat.com/security/cve/CVE-2026-119610
https://nvd.nist.gov/vuln/detail/cve-2026-105467	**8,1**	IBM Qradar	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	IBM QRadar 7.5.0 through 7.5.0 Update Pack 16 Interim Fix 02, and 7.6.0.0 through 7.6.0.5	https://www.ibm.com/support/pages/node/7295450
https://nvd.nist.gov/vuln/detail/cve-2026-97677	**8,1**	IBM Langflow OSS	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	IBM Langflow OSS 1.0.0 through 1.12.2	https://www.ibm.com/support/pages/node/7290694
https://nvd.nist.gov/vuln/detail/cve-2026-95648	**8,1**	C-Prot AppDefense	Improperly Controlled Modification of Dynamically-Determined Object Attributes	C-Prot AppDefense: before 1.0.2729	https://siberguvenlik.gov.tr/guvenlik-bildirimleri/detay/tr-26-1487
https://nvd.nist.gov/vuln/detail/cve-2026-123802	**8,1**	SuperTokens Core	Insufficient Granularity of Access Control	From 11.3.0 until 11.3.8, 11.4.8, 12.0.11, 12.1.2, 12.2.1, and 12.3.1	https://github.com/supertokens/supertokens-core/commit/00a15e045323ba8a566ca6f59b70125b4030ab6c
https://nvd.nist.gov/vuln/detail/cve-2026-12964	**8,0**	DIAEnergie	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	DIAEnergie: before 1.11.01.032.	https://filecenter.deltaww.com/news/download/doc/Delta-PCSA-2026-00017_DIAEnergie%20SQL%20Injection%20Vulnerability_v1.0.pdf
https://nvd.nist.gov/vuln/detail/cve-2026-119474	**7,8**	Liman Render Engine	Incorrect Permission Assignment for Critical Resource	Liman Render Engine: before 1.2-81.	https://siberguvenlik.gov.tr/guvenlik-bildirimleri/detay/tr-26-1489
https://nvd.nist.gov/vuln/detail/cve-2026-114031	**7,8**	Illumio VEN	Incorrect Permission Assignment for Critical Resource	-	https://product-docs-repo.illumio.com/Tech-Docs/Security+Advisories/out/en/security-advisories/insecure-folder-permissions-in-the-windows-ven.html
https://nvd.nist.gov/vuln/detail/cve-2026-109800	**7,7**	SAP Web Dispatcher	Stack-based Buffer Overflow	-	https://me.sap.com/notes/3803832
https://nvd.nist.gov/vuln/detail/cve-2026-124563	**7,7**	D-Link DIR-878	Improper Restriction of Operations within the Bounds of a Memory Buffer	D-Link DIR-878 1.20B05	https://github.com/Zimo-666/DIR-878-cves/tree/main/05-setwansettings-l2tp-pptp-dns-overflow

https://nvd.nist.gov/vuln/detail/cve-2026-93879	**7,5**	Hibernate Validator	Uncontrolled Resource Consumption	-	https://www.ibm.com/support/pages/node/7293301
https://nvd.nist.gov/vuln/detail/cve-2026-90591	**7,5**	NXP ENET-QOS	Out-of-bounds Write	-	https://github.com/zephyrproject-rtos/zephyr/commit/9efd144a4ab0f37311f7b5e5ed0967f5a8d2f910
https://nvd.nist.gov/vuln/detail/cve-2026-89114	**7,5**	SAP NetWeaver AS Java EDM	Missing Authorization	-	https://me.sap.com/notes/3810485
https://nvd.nist.gov/vuln/detail/cve-2026-76973	**7,5**	SAP NetWeaver and ABAP	Integer Overflow or Wraparound	IBM Security Verify Directory 10.0.0 through 10.0.4 and IBM Verify Directory 11.0.0	https://me.sap.com/notes/3789273
https://nvd.nist.gov/vuln/detail/cve-2026-73857	**7,5**	ModSecurity	Out-of-bounds Write	From 3.0.15 until 3.0.17	https://github.com/owasp-modsecurity/ModSecurity/commit/e979a73e89d60cefdf42b41bb38bf1e456d7909f
https://nvd.nist.gov/vuln/detail/cve-2026-124598	**7,5**	GV-Face package	Use of Hard-coded Cryptographic Key	-	https://www.geovision.com.tw/cyber_security.php
https://nvd.nist.gov/vuln/detail/cve-2026-121722	**7,5**	Formidable Forms	Missing Authorization	Formidable Forms Signature Online Contract Automation: from n/a through 2.0.5.	https://patchstack.com/database/wordpress/plugin/forms-signature-formidable-online-contract-automation/vulnerability/wordpress-formidable-forms-signature-online-contract-automation-plugin-2-0-5-broken-access-control-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/cve-2026-121760	**7,5**	weDocs	Missing Authorization	weDocs: from n/a through 2.6.1.	https://patchstack.com/database/wordpress/plugin/wedocs/vulnerability/wordpress-wedocs-plugin-2-6-1-broken-access-control-vulnerability-2?_s_id=cve
https://nvd.nist.gov/vuln/detail/cve-2026-120367	**7,5**	Apache Axis2/Java	Allocation of Resources Without Limits or Throttling	Apache Axis2/Java: through 2.0.1	http://www.openwall.com/lists/oss-security/2026/11/06/26
https://nvd.nist.gov/vuln/detail/cve-2026-120015	**7,5**	SAP Host Agent	Uncontrolled Search Path Element	-	https://me.sap.com/notes/3842766
https://nvd.nist.gov/vuln/detail/cve-2026-119755	**7,5**	Tasmota	Cross-Site Request Forgery (CSRF)	Tasmota through 16.0.0	https://github.com/arendst/Tasmota/commit/1cb7ebcafb0b79f1836d0e9948275f78abc17d7b
https://access.redhat.com/security/cve/CVE-2026-119079	**7,5**	MIT Kerberos 5 (aka krb5)	Incorrect Behavior Order: Early Amplification	MIT Kerberos 5 (aka krb5) 1.11	https://access.redhat.com/security/cve/CVE-2026-119079
https://nvd.nist.gov/vuln/detail/cve-2026-115339	**7,5**	Progress Software WS_FTP Server	Allocation of Resources Without Limits or Throttling	Progress Software WS_FTP Server releases prior to 2025.0.5	https://community.progress.com/s/article/WS-FTP-Server-Service-Pack-November-2026

https://nvd.nist.gov/vuln/detail/cve-2026-112322	**7,5**	MIT Kerberos 5 (aka krb5)	Allocation of Resources Without Limits or Throttling	https://access.redhat.com/security/cve/CVE-2026-112322	
https://nvd.nist.gov/vuln/detail/cve-2026-125704	**7,5**	Gstreamer	Use After Free	-	https://access.redhat.com/security/cve/CVE-2026-125704
https://nvd.nist.gov/vuln/detail/cve-2026-123367	**7,4**	ector Graphics (ThorVG)	Out-of-bounds Write	Prior to 1.1.2	https://github.com/thorvg/thorvg/commit/67680c546d38d817e42eb7583dac8d87a4a319b5
https://nvd.nist.gov/vuln/detail/cve-2026-92864	**7,3**	Hitachi Dynamic Link Manager for AIX	UNIX Symbolic Link (Symlink) Following	Hitachi Dynamic Link Manager for AIX: from 7.4.1-00 before 9.0.4-01; Hitachi Dynamic Link Manager EX for AIX: from 7.4.1-00 before 9.0.4-01.	https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2026-164/index.html
https://nvd.nist.gov/vuln/detail/cve-2026-123484	**7,1**	Crocoblock JetFormBuilder	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	JetFormBuilder: from n/a through 3.6.8.	https://patchstack.com/database/wordpress/plugin/jetformbuilder/vulnerability/wordpress-jetformbuilder-plugin-3-6-8-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/cve-2026-121780	**7,1**	Flying Images.	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Flying Images: from n/a through 2.4.15.	https://patchstack.com/database/wordpress/plugin/nazy-load/vulnerability/wordpress-flying-images-plugin-2-4-15-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/cve-2026-121764	**7,1**	FV Flowplayer Video Player	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	FV Flowplayer Video Player: from n/a through 7.5.56.7212.	https://patchstack.com/database/wordpress/plugin/fv-wordpress-flowplayer/vulnerability/wordpress-fv-flowplayer-video-player-plugin-7-5-56-7212-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/cve-2026-121570	**7,1**	RSVP and Event Management	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	RSVP and Event Management: from n/a through 2.7.17.	https://patchstack.com/database/wordpress/plugin/rsvp/vulnerability/wordpress-rsvp-and-event-management-plugin-2-7-17-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/cve-2026-119505	**7,1**	Welcart e-Commerce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Welcart e-Commerce: from n/a through 2.12.6.	https://patchstack.com/database/wordpress/plugin/usc-e-shop/vulnerability/wordpress-welcart-e-commerce-plugin-2-12-6-cross-site-scripting-xss-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/cve-2026-91760	**7,0**	Hitachi Dynamic Link Manager for Linux	Heap-based Buffer Overflow	Hitachi Dynamic Link Manager for Linux: from 7.5.0-00 before 9.0.5-00.	https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2026-166/index.html

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 One Known Exploited Vulnerability to Catalog	▪ CVE-2026-19868 SonicWall SonicOS SSLVPN Use of Single-factor Authentication Vulnerability	https://www.cisa.gov/news-events/alerts/2026/11/06/cisa-adds-one-known-exploited-vulnerability-catalog
CISA Adds Four Known Exploited Vulnerabilities to Catalog	▪ CVE-2026-102895 GPUStack Improper Authentication Vulnerability ▪ CVE-2026-116779 SignalWire FreeSwitch Code Injection Vulnerability ▪ CVE-2026-123158 OpenBSD OpenSSH Unexpected Status Code or Return Value Vulnerability ▪ CVE-2026-123218 IBM Aspera Faspex Incorrect Authorization Vulnerability	https://www.cisa.gov/news-events/alerts/2026/11/09/cisa-adds-four-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
ARTEX AI Hacking Framework Found on 1,465 Public Servers, Some Hosting Cyberattack Tools	https://cybersecuritynews.com/artex-ai-hacking-framework/
Hackers Use ARTEX AI to Find GitHub Secrets and Steal Azure Key Vault Data in Just 5 Minutes	https://cybersecuritynews.com/hackers-use-artex-ai/
ARTEX AI Agents Steal 190,000 Gaming Credentials and Hundreds of Apple Code-Signing Certificates	https://cybersecuritynews.com/artex-ai-agents/
Microsoft Warns Fake Game Downloads Are Secretly Monetizing Windows PCs	https://cybersecuritynews.com/microsoft-warns-fake-game-downloads/
New Dark Project Ransomware Group Offers Hackers 80% Commission to Expand Cyberattacks	https://cybersecuritynews.com/new-dark-project-ransomware-group/
ARTEX AI Agent Escapes Research Sandbox and Accesses WorkOS Customer Records	https://cybersecuritynews.com/workos-customer-records-exposed/
NVIDIA Investigates Suspected Chinese Spy Operation Targeting CEO Jensen Huang	https://cybersecuritynews.com/nvidia-investigates-chinese-spy-operation/
Claude AI Accidentally Deletes Law Professor’s Entire Syllabus and One Year of Lecture Notes	https://cybersecuritynews.com/claude-ai-deletes-law-professors-entire-syllabus/
U.S. Agencies Warn of Hackers Targeting Industrial Refrigeration to Disrupt Food and Medicine Storage	https://cybersecuritynews.com/hackers-targeting-industrial-refrigeration-systems/
Hackers Use ARTEX AI to Steal Azure Key Vault Secrets Just 5 Minutes After Scanning GitHub	https://cybersecuritynews.com/artex-ai-azure-key-vault-secrets/
Hackers Hijack 10 npm Packages to Spread PolinRider Malware Using Ethereum Blockchain	https://cybersecuritynews.com/hackers-hijack-10-npm-packages-to-spread-polinrider-malware-using-ethereum-blockchain/
Jailbroken DeepSeek AI Agent Breaches European Telecom and Accesses Millions of Patient Records	https://cybersecuritynews.com/jailbroken-deepseek-ai-agent-breach/
GhostAction Hackers Compromise 500+ GitHub Accounts to Steal AWS, OpenAI, and Cloud Credentials	https://cybersecuritynews.com/ghostaction-github-account-compromise/

Σύντομη περιγραφή / Τίτλος	URL
RevStealer Uses 100+ Domains and Hijacked YouTube Channels to Spread Credential-Stealing Malware	https://cybersecuritynews.com/revstealer-uses-100-domains/

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
Hackers Could Bypass ChatGPT Lockdown Mode to Steal Conversations Without Users Knowing	https://cybersecuritynews.com/chatgpt-lockdown-mode-bypass/
Mirax Android RAT Hijacks Phones Through Streaming-App Ads to Steal Banking Credentials and Drain Accounts	https://cybersecuritynews.com/mirax-android-rat/
Anthropic's Claude Code Reportedly Leaks User Email Addresses Through HTTP User-Agent Headers	https://cybersecuritynews.com/claude-code-leaks-user-email/
Hackers Deploy ArmorSteal Malware Through Fake Software Downloads to Steal Credentials and Mine Crypto	https://cybersecuritynews.com/armorsteal-malware/

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
Claude Dispatch Flaw Lets Malicious Browser Extensions Run Code on Connected Computers	https://cybersecuritynews.com/claude-dispatch-vulnerability/
Storm-2603 Hackers Exploit SharePoint ToolShell Flaws to Hide Fileless Backdoor and Launch Ransomware Attack	https://cybersecuritynews.com/storm-2603-hackers/
Hackers Launch 240,000 Attempts to Exploit a WordPress Core Flaw That Allows Remote Code Execution	https://cybersecuritynews.com/240000-wordpress-exploit-attempts/
Critical React Server Components Flaw Lets Hackers Execute Code Remotely Without Authentication	https://cybersecuritynews.com/react-server-components-vulnerability-patch/
Hackers Begin Exploiting OpenSSH SSHole Authentication Bypass Vulnerability	https://cybersecuritynews.com/openssh-sshole-flaw-exploited/
Veeam Warns Critical 9.8 Linux Kernel Flaw Could Crash Backup Appliances and Disrupt Recovery Operations	https://cybersecuritynews.com/veeam-warns-critical-linux-kernel-flaw/
ModSecurity Patches Two High-Severity Flaws Allowing WAF Bypass and Potential Remote Code Execution	https://cybersecuritynews.com/modsecurity-patches-two-high-severity-flaws/
Terminal2Shell: 55-Year-Old ‘Zero-Day’ Dating Back to 1971 Claims to Affect Billions of Devices	https://cybersecuritynews.com/terminal2shell-55-year-old-zero-day/
Google Chrome 0-Day Vulnerability in the Wild to Execute Malicious Code Remotely	https://cybersecuritynews.com/google-chrome-0-day-exploited/

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
Notepad++ 8.9.9 Released With Fixes for 6 Vulnerabilities Allowing Plugin Command Execution	https://cybersecuritynews.com/notepad-8-9-9-released/
N-able Takes N-central Servers Offline Worldwide After 33 0-Day Vulnerabilities and Able2Shell Exploits	https://cybersecuritynews.com/n-able-takes-n-central-servers-offline/

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
Claude Code's "Yes, and Don't Ask Again" Option Can Leak Passwords and API Keys to GitHub	https://cybersecuritynews.com/claude-codes-yes-and-dont-ask-again/
SonicWall Warns of Potential In-the-Wild Exploitation of SSLVPN Flaw That Bypasses MFA	https://cybersecuritynews.com/sonicos-sslvpn-vulnerability-exploited/
CISA Warns Two Critical 9.0 Flaws in PowerSYSTEM Center Allow Unauthorized Access and SQL Injection	https://cybersecuritynews.com/cisa-warns-critical-flaws-in-powersystem-center/
Hackers Exploit Plex2Shell Flaws to Take Over Plex Media Servers and Deploy Crypto Miners	https://cybersecuritynews.com/hackers-exploit-plex2shell-flaws/
Researchers Uncover NotC2 AI-Powered C2 Framework That Hides Malicious Commands Inside AWS Services	https://cybersecuritynews.com/notc2-ai-powered-c2-framework/
CISA Warns of SonicWall SonicOS SSLVPN Vulnerability Exploited in Attacks	https://cybersecuritynews.com/sonicwall-sonicos-sslvpn-vulnerability-exploited/

Σύντομη περιγραφή / Τίτλος	URL
Google Gemini Safety Bypass Lets Users Download AI-Generated Images That Its Own Filters Blocked	https://cybersecuritynews.com/google-gemini-safety-bypass-ai-generated-images/
Hackers Used Default admin:admin Credentials to Exploit ForgeRock RCE and Remotely Unlock Cars	https://cybersecuritynews.com/forgerock-attack-chain/
Anubis Ransomware Hackers Deploy New Lindnor Backdoor and 13 Security-Killing Tools in U.S. Attack	https://cybersecuritynews.com/anubis-ransomware-lindnor-backdoor/
New Abe Office Malware Bypasses Chrome App-Bound Encryption to Steal Browser Passwords and Cookies	https://cybersecuritynews.com/abe-office-malware/
Hackers Breach Fireworks AI Through Third-Party Cloud Provider to Steal Customer Data	https://cybersecuritynews.com/fireworks-ai-data-breach/

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 Deception Technology Solutions in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-deception-technology/

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/