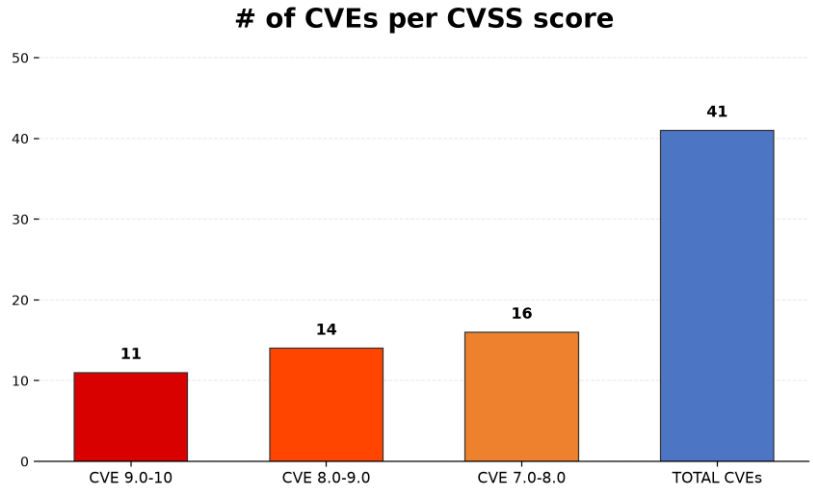
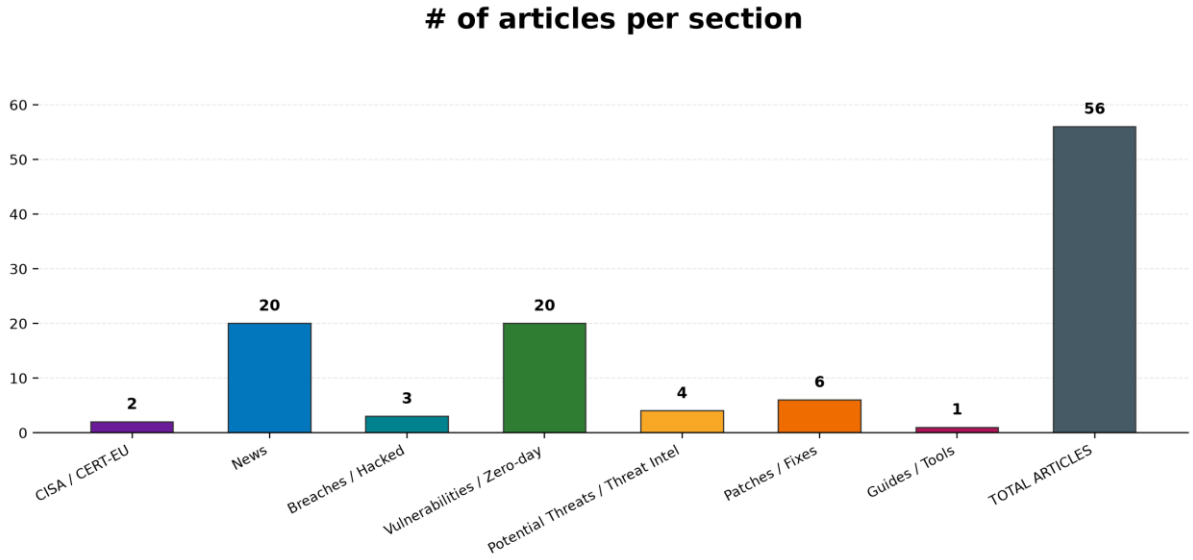
Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 24/10/2026 - 27/10/2026





Contents

Common Vulnerabilities and Exposures (CVEs) 3
CISA/CERT-EU Alerts & Advisories 7
News 8
Breaches / Compromised / Hacked 9
Vulnerabilities / Flaws / Zero-day 9
Patches / Updates / Fixes 10
Potential threats / Threat intelligence 11
Guides / Tools 11
References 12
Annex – Websites with vendor specific vulnerabilities 13

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 v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-116508	10,0	TOTOLINK A950RG	Improper Restriction of Operations within the Bounds of a Memory Buffer; Stack-based Buffer Overflow	4.1.2cu.5268_B20221104	https://gist.github.com/H3rmesk1t/ad72def4ccc232757d4cbabf45da72cb https://vuldb.com/cve/CVE-2026-116508 https://vuldb.com/submit/1022557 https://vuldb.com/vuln/426406 https://vuldb.com/vuln/426406/cti https://www.totolink.net/			
CVE-2026-65145	10,0	NVIDIA NeMo Agent Toolkit	Missing Authentication for Critical Function	1.0 to 1.8.0	https://github.com/NVIDIA/product-security/tree/main/2026/5912 https://nvd.nist.gov/vuln/detail/CVE-2026-65145 https://www.cve.org/CVERecord?id=CVE-2026-65145			
CVE-2026-110720	9,9	Consul-k8s	Incorrect Authorization	0.42.0 and later	https://discuss.hashicorp.com/t/hcsec-2026-50-consul-k8s-vulnerable-to-a-cross-namespace-authorization-bypass-in-component-acl-binding-rules/77915	none	no	total
CVE-2026-117532	9,8	REDAXO core	Improper Authentication	before 5.21.4	https://github.com/redaxo/core/security/advisories/GHSA-px8f-whj8-hrpg https://www.vulncheck.com/advisories/redaxo-core-5.3.0-before-5.21.4-authentication-bypass-via-history-plugin			
CVE-2026-18450	9,8	X12SPI	Missing Authentication for Critical Function	01.07.20	https://www.supermicro.com/en/support/security_BMC_IPMI_Oct_2026_1			
CVE-2026-76934	9,8	JP1/Automatic Job Management System	Stack-based Buffer Overflow	before 13-50-31; before 13-50-31.	https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2026-140/index.html			
CVE-2026-82116	9,8	HiRDB	Missing Authentication for Critical Function	before 10-12-01; from 09-00 through 09-66-22; from 09-00 through 09-66; from 09-02 through 09-66-22; from 09-00 through 09-66-	https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2026-148/index.html			
CVE-2026-86574	9,8	JP1/Base	Heap-based Buffer Overflow	before 12-50-54.	https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2026-156/index.html			
CVE-2026-92885	9,8	The Qode Membership plugin for WordPress	Improper Authentication	up to, and including, 2.0.6.2	https://themeforest.net/item/bridge-creative-multipurpose-wordpress-theme/7315054 https://www.wordfence.com/threat-intel/vulnerabilities/id/26bca6c2-0999-4cf6-9c4e-ddaf528ef808?source=cve			
CVE-2026-86575	9,4	JP1 Products	Stack-based Buffer Overflow	before 13-50-31; before 12-50-54.	https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2026-155/index.html			
CVE-2026-112362	9,1	@fastify/express	Interpretation Conflict	In versions 4.0.5 through 4.0.8	https://cna.openjsf.org/security-advisories.html https://github.com/fastify/fastify-express/security/advisories/GHSA-6h42-57hg-9746			
CVE-2026-112438	8,8	macOS		prior to 15.8.2; prior to 26.7.2; prior to 27.2	https://support.apple.com/en-us/149521 https://support.apple.com/en-us/149522 https://support.apple.com/en-us/149523	none	no	total

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-112623	8,8	A	Use After Free	prior to 27.2; prior to 26.7.2	https://support.apple.com/en-us/149227 https://support.apple.com/en-us/149230 https://support.apple.com/en-us/149521 https://support.apple.com/en-us/149526 https://support.apple.com/en-us/149527	none	no	total
CVE-2026-116201	8,8	Snipe-IT	Authentication Bypass by Capture-replay	before 8.5.0	https://github.com/grokability/snipe-it/security/advisories/GHSA-w49g-f2jc-gxhg https://www.vulncheck.com/advisories/snipe-it-before-8.5.0-saml-assertion-replay-via-race-condition			
CVE-2026-116738	8,8	VMime	Stack-based Buffer Overflow	through 0.9.2	https://github.com/kisli/vmime https://github.com/kisli/vmime/blob/v0.9.2/src/vmime/utility/encoder/uuEncoder.cpp#L185-L190 https://github.com/kisli/vmime/commit/e85925eddc638939f0eeb7ee55ec047d04a760d8 https://github.com/kisli/vmime/pull/363 https://hackmd.io/@haindpwn/vmime-uuencode-decoder-oob-write https://www.vulncheck.com/advisories/vmime-through-0.9.2-stack-based-buffer-overflow-via-uuencode-decoder			
CVE-2026-116748	8,8	Transmission	Permissive Cross-domain Security Policy with Untrusted Domains	before 4.1.3	https://github.com/transmission/transmission https://github.com/transmission/transmission/blob/4.1.2/libtransmission/rpc-server.cc#L560 https://github.com/transmission/transmission/commit/c6a1bd2017a0fea9c956737c213f23e4b0f7929e https://github.com/transmission/transmission/pull/8938 https://github.com/transmission/transmission/releases/tag/4.1.3 https://joshua.hu/transmission-cors-rpc-csrf-rce-drive-by-exploit			
CVE-2026-116836	8,8	airMAX M	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	prior to 6.3.26	https://uisp.community.ui.com/releases/Security-Advisory-Bulletin-071/7d4d42cf-09e4-44d3-9c19-649cac8c6af3			
CVE-2026-116843	8,8	Mistral Vibe	Inclusion of Functionality from Untrusted Control Sphere	before 3.0.3	https://github.com/mistralai/mistral-vibe/blob/v2.24.1/vibe/core/worktree.py#L303-L317 https://github.com/mistralai/mistral-vibe/commit/7bb48f213ac677f943d5c791199ed3dddf302f00 https://github.com/mistralai/mistral-vibe/issues/997 https://github.com/mistralai/mistral-vibe/releases/tag/v3.0.3 https://www.vulncheck.com/advisories/mistral-vibe-before-3.0.3-rce-via-git-filter-drivers-in-worktree-mode			
CVE-2026-117536	8,8	REDAXO	Cross-Site Request Forgery (CSRF)	before 5.21.3	https://github.com/redaxo/core/security/advisories/GHSA-mrrj-4f5x-j958 https://www.vulncheck.com/advisories/redaxo-before-5.21.3-csrf-token-bypass-via-users-users-privilege-escalation			
CVE-2026-65220	8,8	the BMC IPMI implementation	Improper Privilege Management	01.07.20	https://www.supermicro.com/en/support/security_BMC_IPMI_Oct_2026_1			
CVE-2026-75891	8,8	The Kirki plugin for WordPress; all	Deserialization of Untrusted Data	up to, and including, 6.2.5	https://plugins.trac.wordpress.org/changeset/3677965/kirki https://www.wordfence.com/threat-intel/vulnerabilities/id/aecfea73-97fc-48c3-bf1b-5314077739b5?source=cve			
CVE-2026-115924	8,6	Rembg	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Prior to 2.0.82	https://github.com/danielgatis/rembg/commit/b2758c6b39bb2b02df90a0312811033947698 4d3 https://github.com/danielgatis/rembg/releases/tag/v2.0.82 https://github.com/danielgatis/rembg/security/advisories/GHSA-gr6x-7v33-6gmg			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-65119	8,4	NVIDIA TensorRT-LLM for any platform; KvCacheAwareRouter tokenizer loading, where an attacker	Inclusion of Functionality from Untrusted Control Sphere	1.3.0rc24	https://github.com/NVIDIA/product-security/tree/main/2026/5883 https://nvd.nist.gov/vuln/detail/CVE-2026-65119 https://www.cve.org/CVERecord?id=CVE-2026-65119			
CVE-2024-58400	8,2	llama.cpp	Improper Validation of Array Index	prior to b3701	https://github.com/ggml-org/llama.cpp/blob/b3681/examples/server/server.cpp#L789 https://github.com/ggml-org/llama.cpp/commit/eae597182cb61bbde0b26e7cec5999d28b9327fe https://github.com/ggml-org/llama.cpp/commit/faf69d4237c9ae4d7f572b4674d1002463e8acd3 https://github.com/ggml-org/llama.cpp/pull/9359 https://github.com/ggml-org/llama.cpp/releases/tag/b3701 https://www.vulncheck.com/advisories/llama-cpp-before-b3701-out-of-bounds-read-in-llama-decode-via-token-ids			
CVE-2026-116747	8,1	Kener	Use of Hard-coded Cryptographic Key	before 4.1.10	https://github.com/rajnandan1/kener https://github.com/rajnandan1/kener/blob/v4.1.9/src/lib/server/controllers/commonController.ts#L44-L55 https://github.com/rajnandan1/kener/commit/ff636483544c926eab5b5e3e26b811c0f52bcaf8 https://github.com/rajnandan1/kener/issues/871 https://github.com/rajnandan1/kener/releases/tag/v4.1.10 https://www.vulncheck.com/advisories/kener-3.0.0-before-4.1.10-authentication-bypass-via-hardcoded-fallback-jwt-secret			
CVE-2026-116723	7,8	FLTK	Stack-based Buffer Overflow	through 1.4.5	https://github.com/fltk/fltk https://github.com/fltk/fltk/blob/release-1.4.5/src/Fl_BMP_Image.cxx#L255-L265 https://github.com/fltk/fltk/commit/3a049d8262dc759cf9737339420e8457e24c0cb1 https://github.com/fltk/fltk/issues/1632 https://hackmd.io/@haindpwn/fltk-bmp-image-stack-heap-overflow https://www.vulncheck.com/advisories/fltk-through-1.4.5-stack-buffer-overflow-via-fl-bmp-image-colors-used-field			
CVE-2026-47486	7,8	NVIDIA PhysX for all platforms	Out-of-bounds Write	0.0 to 0.4.1.2	https://github.com/NVIDIA/product-security/tree/main/2026/5915 https://nvd.nist.gov/vuln/detail/CVE-2026-47486 https://www.cve.org/CVERecord?id=CVE-2026-47486			
CVE-2026-100164	7,5	Rolantis Information Technologies Tourism Industry and Trade Co	Observable Response Discrepancy	before 4.8.	https://siberguvenlik.gov.tr/guvenlik-bildirimleri/detay/tr-26-1406			
CVE-2026-106174	7,5	Fortinet FortiOS	Improper Locking	7.6.4 through 7.6.6	https://fortiguard.fortinet.com/psirt/FG-IR-26-181	none	yes	partial

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-116587	7,5	Go JOSE; Go, including support for JSON Web Encryption (JWE), JSON Web Signature (JWS), and JSON Web Token (JWT) standards	Inefficient Algorithmic Complexity; Allocation of Resources Without Limits or Throttling	Prior to 4.1.6; 1.24 and later	https://github.com/go-jose/go-jose/commit/a0111f82742fa92bceec9ede40845e73319e6230 https://github.com/go-jose/go-jose/releases/tag/v4.1.6 https://github.com/go-jose/go-jose/security/advisories/GHSA-mgcc-cww5-fp2g			
CVE-2026-116871	7,5	Semantic MediaWiki	Uncontrolled Recursion	before 7.3.1	https://github.com/SemanticMediaWiki/SemanticMediaWiki/commit/756492002752f937a9e115e14330b1181bd8c60c https://github.com/SemanticMediaWiki/SemanticMediaWiki/commit/e642f38c708dee7da5e885b8d40be8ffc56f3e87 https://github.com/SemanticMediaWiki/SemanticMediaWiki/security/advisories/GHSA-f8vw-wvm6-h2qq https://www.vulncheck.com/advisories/semantic-mediawiki-3.0.0-before-7.3.1-uncontrolled-recursion-via-special-ask			
CVE-2026-41020	7,5	Eaton easyE4	Authentication Bypass by Capture-replay	prior to 2.46	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/eaton-va-2026-1017.pdf			
CVE-2026-92546	7,5	Keepnet Labs Cybersecurity Inc	Authentication Bypass by Spoofing	before 0ef61f2e.	https://siberguvenlik.gov.tr/guvenlik-bildirimleri/detay/tr-26-1408			
CVE-2026-65219	7,4	the BMC RAKP+ implementation	Incorrect Behavior Order	1.07.20	https://www.supermicro.com/en/support/security_BMC_IPMI_Oct_2026_1			
CVE-2026-116620	7,3	Tencent RapidJSON	Improper Restriction of Operations within the Bounds of a Memory Buffer; Out-of-bounds Read	up to 1.1.0.	https://github.com/Tencent/rapidjson/ https://github.com/Tencent/rapidjson/issues/2401 https://vuldb.com/cve/CVE-2026-116620 https://vuldb.com/submit/1024236 https://vuldb.com/vuln/426552 https://vuldb.com/vuln/426552/cti			
CVE-2026-116623	7,3	code-projects Simple Content Management System	Missing Authorization; Incorrect Authorization	1.0	https://code-projects.org/ https://github.com/YoonSunWoo02/CVE-simple-cms-broken-access-control https://vuldb.com/cve/CVE-2026-116623 https://vuldb.com/submit/1024407 https://vuldb.com/vuln/426553 https://vuldb.com/vuln/426553/cti			
CVE-2026-109995	7,2	The Advanced Views – Display Framework for Gutenberg & Elementor plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 3.9.6	https://plugins.trac.wordpress.org/browser/acf-views/tags/3.9.6/src/Cpt/Data_Vendors/Base/Fields/Custom_Field.php#L70 https://plugins.trac.wordpress.org/browser/acf-views/tags/3.9.6/src/Cpt/Data_Vendors/Wp/Fields/Comment/Comment_Content_Field.php#L27 https://plugins.trac.wordpress.org/browser/acf-views/tags/3.9.6/src/Cpt/Data_Vendors/Wp/Fields/Comment/Comment_Content_Field.php#L50 https://plugins.trac.wordpress.org/browser/acf-views/tags/3.9.7/src/Cpt/Data_Vendors/Wp/Fields/Comment/Comment_Content_Field.php https://www.wordfence.com/threat-intel/vulnerabilities/id/57ccea1b-d579-444e-a7e6-ae1ed218ea59?source=cve			

URL ευπάθειας (NIST NVD)	CVSS v3.1	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL οδηγιών αντιμετώπισης	Exploitation	Automatable	Technical Impact
CVE-2026-111820	7,2	The Analytics Insights – Google Analytics Dashboard for WordPress plugin for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	up to, and including, 6.3.12	https://plugins.trac.wordpress.org/browser/analytics-insights/trunk?rev=3755146 https://www.wordfence.com/threat-intel/vulnerabilities/id/2164289e-dc9a-4659-85fe-0818092466c4?source=cve			
CVE-2026-16521	7,2	MBD-X12STW-F	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01.02.08	https://www.supermicro.com/en/support/security_BMC_IPMI_Oct_2026_2			
CVE-2026-65211	7,2	MBD-X12SPI	Improper Authentication	01.07.20	https://www.supermicro.com/en/support/security_BMC_IPMI_Oct_2026_1			
CVE-2026-24269	7,1	NVIDIA TensorRT-LLM	Server-Side Request Forgery (SSRF)	1.3.0rc24	https://github.com/NVIDIA/product-security/tree/main/2026/5883 https://nvd.nist.gov/vuln/detail/CVE-2026-24269 https://www.cve.org/CVERecord?id=CVE-2026-24269			

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
Critical Vulnerabilities in PHP Require Immediate Patching | CISA	• CVE-2026-109618 • CVE-2026-109619	https://cisa.gov/news-events/alerts/2026/10/21/critical-vulnerabilities-php-require-immediate-patching
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA	CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog and updated the PHP Alert, Critical Vulnerabilities in PHP Require Immediate Patching :	https://cisa.gov/news-events/alerts/2026/10/26/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
Vendor Key Leak Puts Data of 238,000 Denver Health Plan Members at Risk	https://securityweek.com/vendor-key-leak-puts-data-of-238000-denver-health-plan-members-at-risk
Attackers Exploit Teams External Chat to Breach Organizations in Un-der	https://infosecurity-magazine.com/news/exploit-teams-chat-breach
Unexplained DreamHost Incident Prompts Email, FTP Password Resets	https://securityweek.com/unexplained-dreamhost-incident-prompts-email-ftp-password-resets
Keystone to Destroy 18,835 Hardware Wallets After Hackers Steal De-vice Verification Key	https://thehackernews.com/2026/10/keystone-to-destroy-18835-hardware.html
Copenhagen University Breach Compromises Data on Half a Million People	https://infosecurity-magazine.com/news/copenhagen-university-data-breach
Hackers Hijack AI Pentesting Agents to Install Backdoors and Steal API Keys	https://cybersecuritynews.com/ai-pentesting-agents
Risks Spelled Out for Anthropic Investors Include Possible Harms From Runaway AI	https://securityweek.com/risks-spelled-out-for-anthropic-investors-include-possible-harms-from-runaway-ai
First ISC2 AI Security Certification Expected for Early 2027	https://infosecurity-magazine.com/news/first-isc2-ai-security
This is Fine: What NetScaler Zero-Days Tell Us About the New Normal	https://securityweek.com/this-is-fine-what-netscaler-zero-days-tell-us-about-the-new-normal
Dead Popcorn Time Updater Put Millions of Computers at Risk of Take-over	https://securityweek.com/dead-popcorn-time-updater-put-millions-of-computers-at-risk-of-takeover
Watchdog Warns Police and Fire Service Must Urgently Improve Cyber-secu	https://infosecurity-magazine.com/news/watchdog-police-fire-service
Your AI Stack Is Exposed. Make It Unreachable.	https://darkreading.com/application-security/your-ai-stack-is-exposed-make-it-unreachable-
Hacker Uses AI to Breach 90 South Korean Organizations and Steal 8.2 Million Records	https://cybersecuritynews.com/hacker-uses-ai-to-breach-organizations
Alibaba's Qwen AI Said It Wouldn't Execute Commands, Then Tried to Send Data to China	https://cybersecuritynews.com/alibabas-qwen-ai-tried-to-send-data-to-china
DreamHost Forces Email and FTP Password Resets Following Unex-plained Security Incident	https://cybersecuritynews.com/dreamhost-forces-email-and-ftp-password-resets
OpenAI Unveils GPT-6.1 Terra, a Faster AI Model With Critical Cyberse-curity Capabilities	https://cybersecuritynews.com/openai-unveils-gpt-6-1-terra
Privacy Policy	https://cybersecuritynews.com/privacy-policy-2
Article Publication and Retention Policy	https://cybersecuritynews.com/terms-of-service
About Us	https://cybersecuritynews.com/about-us
Hackers Infect 953 Online Stores With Malicious JavaScript That Evades Security Scanners	https://cybersecuritynews.com/hackers-infect-953-online-stores

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
Energy giant ENGIE discloses data breach affecting customers	https://bleepingcomputer.com/news/security/energy-giant-engie-discloses-data-breach-affecting-customers
University of Copenhagen Data Breach Exposes 525,000 People's Personal Data, Including Phone Numbers	https://cybersecuritynews.com/university-of-copenhagen-data-breach
University of Copenhagen data breach exposes data of 525,000 people	https://bleepingcomputer.com/news/security/university-of-copenhagen-data-breach-exposes-data-of-525-000-people

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
Microsoft Authenticator Flaw Let Permissionless Android Apps Steal Work Account Tokens	https://thehackernews.com/2026/10/microsoft-authenticator-flaw-let.html
iOS, macOS 27.2 Patch 286 Bugs; Fix for Exploited Flaw Backported to iOS 18	https://securityweek.com/ios-macos-27-2-patch-286-bugs-fix-for-exploited-flaw-backported-to-ios-18
From Vulnerability Management to Vulnerability Elimination	https://darkreading.com/application-security/from-vulnerability-management-to-vulnerability-elimination
Critical HashiCorp Consul Kubernetes Flaw Allows Attackers to Gain Elevated Privileges	https://cybersecuritynews.com/hashicorp-consul-kubernetes-vulnerability
Apple iOS 27.2 Released With Fixes for 163 Vulnerabilities, Including Fix for Critical WebKit RCE	https://cybersecuritynews.com/apple-ios-27-2-released
OpenAI Compaction Flaw Let Researchers Bypass Hidden Reasoning Protections	https://thehackernews.com/2026/10/openai-compaction-flaw-let-researchers.html
CISA confirms PHP2Shell vulnerabilities now exploited in attacks	https://bleepingcomputer.com/news/security/cisa-confirms-php2shell-vulnerabilities-now-exploited-in-attacks
Maritime Coalition Launches Free Vulnerability Database for Ship and Port Systems	https://securityweek.com/maritime-coalition-launches-free-vulnerability-database-for-ship-and-port-systems
CISA Confirms Active Exploitation of Two PHP2Shell Flaws Enabling Remote Code Execution	https://thehackernews.com/2026/10/cisa-confirms-active-exploitation-of.html
PHP Issues Second Windows Security Update in Five Days to Fix Brotli Code Execution Flaw	https://thehackernews.com/2026/10/php-issues-second-windows-security.html
Critical 'HTTP2Shell' Brotli vulnerability triggers emergency patches	https://bleepingcomputer.com/news/security/critical-http2shell-brotli-vulnerability-triggers-emergency-patches
PHP Releases New Windows Build Security Updates to Fix Critical HTTP2Shell Vulnerability	https://cybersecuritynews.com/php-http2shell-vulnerability

Σύντομη περιγραφή / Τίτλος	URL
Weekly Recap: This2Shell, That2Shell, Everything's an RCE? Rogue AI, Supply Chain Chaos and More	https://thehackernews.com/2026/10/weekly-recap-this2shell-that2shell.html
Microsoft Issues Emergency Patch Update for Critical .NET Buffer Overf	https://infosecurity-magazine.com/news/microsoft-patch-update-net-flaw
Two Critical Wasmtime Flaws Could Let Malicious WebAssembly Modules Escape Sandboxes	https://thehackernews.com/2026/10/two-critical-wasmtime-flaws-could-let.html
Node2Shell: Brotli Flaw Triggers Patching Across Microsoft, Node.js, Python Packages	https://securityweek.com/node2shell-brotli-flaw-triggers-patching-across-microsoft-node-js-python-packages
Blue Initiative Offers Maritime Sector a Dedicated Vulnerability Repos	https://infosecurity-magazine.com/news/blue-initiative-maritime
PHP2Shell security flaws now sucessfully exploited in the wild	https://bleepingcomputer.com/news/security/php2shell-security-flaws-now-sucessfully-exploited-in-the-wild
PHP Publishes Mitigation Advice for New RCE Flaw	https://infosecurity-magazine.com/news/php-publishes-mitigation-advice
HTTP2Shell Vulnerability Extends Beyond HTTP, Affecting .NET, FFmpeg, ClickHouse, and Apache Arrow	https://cybersecuritynews.com/http2shell-vulnerability

Patches / Updates / Fixes

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

Σύντομη περιγραφή / Τίτλος	URL
HPE Patches Dozens of Critical Flaws in Networking Products	https://securityweek.com/hpe-patches-dozens-of-critical-flaws-in-networking-products
Apple backports CoreGraphics zero-day patches to older iPhones	https://bleepingcomputer.com/news/apple/apple-backports-coregraphics-zero-day-patches-to-older-iphones
Apple Released Patches for Exploited CoreGraphics 0-day Vulnerability for Older iPhones	https://cybersecuritynews.com/apple-fix-for-coregraphics-0-day-flaw
Microsoft releases emergency .NET patches for critical Brotli flaw	https://bleepingcomputer.com/news/microsoft/microsoft-releases-emergency-net-patches-for-critical-brotli-flaw
Linux Flaws Exposed Before Fixes as Root Exploit Goes Public	https://infosecurity-magazine.com/news/linux-flaws-exposed-before-fixes
Unpatched Tailscale SSH Flaws Could Let a Hacked Device Reach Root on Other Servers	https://thehackernews.com/2026/10/unpatched-tailscale-ssh-flaws-could-let.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
Lazarus Abuses South Korean Security Software to Deploy Malware Us-ing Post-Quantum Encryption	https://thehackernews.com/2026/10/lazarus-abuses-south-korean-security.html
953 Online Stores Infected in Long-Lasting Malware Campaign	https://securityweek.com/953-online-stores-infected-in-long-lasting-malware-campaign
Microsoft Teams to Use AI for Detecting Phishing Attacks Using Teams Conversations	https://cybersecuritynews.com/microsoft-teams-ai-detection
Researchers Push Over 2 Million Updates to Remotely Disable Popcorn Time Updater That Could Fuel a Botnet	https://thehackernews.com/2026/10/researchers-push-over-2-million-updates.html

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 10 Best Confidential Computing Platforms in 2026 [Ranked & Scored]	https://cybersecuritynews.com/best-confidential-computing-platforms

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/