CNCS Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança

TLP:CLEAR

9 de abril de 2026

Boletim do Observatório de Cibersegurança do CNCS

N.º 1/2026

Destaques[1]

- Após a aprovação do novo Regime Jurídico da Cibersegurança em Portugal, segue-se a publicação da consulta pública do seu projeto de regulamento; a União Europeia (UE) começa o ano com várias iniciativas para reforçar a cibersegurança, em particular a cadeia de fornecimento.

- Grupos hacktivistas pró-russos procuraram, no último ano, comprometer sistemas operacionais de infraestruturas críticas; a indústria de defesa europeia e ONGs estrangeiras foram alvos de campanhas de ciberespionagem, num trimestre em que foi identificada uma das primeiras campanhas de ciberespionagem orquestradas com IA generativa e supervisão humana limitada;

- Grupo de cibercrime regressa com nova variante de *ransomware*; foram exploradas vulnerabilidades em *routers* industriais para campanhas de *smishing*; foi identificado novo *malware* que se dissimula em imagens digitais para distribuir *malware* e *infostealers*; novo *kit phishing-as-a-service* visa setor bancário europeu e plataformas de criptomoedas;

- Relatório anual dos serviços diplomáticos da UE sobre incidentes de desinformação e operações de informação estrangeiras identifica centenas de incidentes e apresenta abordagem estruturada para lutar contra ações de manipulação de informação por parte de atores maliciosos.

[1] Os dados aqui apresentados foram recolhidos em fontes abertas, tendo sido classificados, avaliados e priorizados de acordo com uma metodologia que inclui a ponderação de variáveis tais como os setores, geografia, impacto organizacional, inovação ao nível das táticas, técnicas e procedimentos (TTPs) e acionabilidade. Comentários e sugestões devem ser enviados para: observatorio [at] cncs [dot] gov [dot] pt .

Políticas públicas e direito[2]

Após a aprovação do novo Regime Jurídico da Cibersegurança em Portugal, foi submetido a consulta pública o seu projeto de regulamento: O Decreto-Lei n.º 125/2025, de 4 de dezembro, transpõe a Diretiva (UE) 2022/2555, abrange 17 setores de atividade e a administração pública, adotando uma abordagem transversal à cibersegurança, com exigências proporcionais à dimensão e criticidade de cada entidade[3]. O projeto de regulamento, que está em consulta pública até dia 22 de abril, vem estabelecer os termos de aplicação de algumas das disposições do regime, nomeadamente as regras de funcionamento da plataforma eletrónica e as medidas de cibersegurança mínimas e níveis de conformidade que devem ser cumpridas pelas entidades[4]. #NIS2

Publicada nova *toolbox* para reforçar a segurança da cadeia de fornecimento das TIC dos Estados-Membros da UE: Esta *toolbox*, publicada a 13 de fevereiro de 2026, define uma abordagem comum à identificação, avaliação e mitigação de riscos de cibersegurança nas cadeias de fornecimento das TIC com vista ao reforço da segurança dos Estados-Membros, como disposto no artigo 22.º da Diretiva NIS 2. Este documento identifica 11 cenários de risco, com origem em ações maliciosas, erro humano e falhas técnicas, e catástrofes naturais. Recomenda ainda a adoção de 7 medidas de mitigação, incluindo medidas com vista à redução da dependência de fornecedores considerados de alto risco[5]. #NIS2 #fornecedores-de-alto-risco

Comissão apresenta proposta de revisão do Cybersecurity Act: Dez anos depois da publicação do regulamento Cybersecurity Act, a Comissão propôs uma atualização do quadro de certificação em matéria de cibersegurança, o reforço das atribuições e competências da ENISA e a introdução de um mecanismo de segurança da cadeia de fornecimento a nível da UE. Se este último mecanismo for adotado, a Comissão passa a poder excluir fornecedores de alto risco em vários contextos, incluindo a participação em fóruns de definição de medidas técnicas de cibersegurança, de atividades financiadas por programas da UE, dos mercados da certificação em cibersegurança e contratos públicos[6]. #fornecedores-de-alto-risco #certificação #ENISA

Conselho da UE voltou a impor sanções a organizações e indivíduos responsáveis por ações maliciosas no ciberespaço da UE: No quadro de instrumentos para a ciberdiplomacia conjunta da UE, foram aplicadas sanções, em março de 2026, a duas entidades sediadas na República Popular da China, uma entidade iraniana e duas pessoas de nacionalidade chinesa. Das várias ações que justificaram estas sanções constam ações de intrusão, ciberespionagem e operações de influência, e comprometimento da cadeia de fornecimento de dispositivos de IoT[7].

[2] A informação recolhida e analisada nesta subsecção abrange o período correspondente ao primeiro trimestre de 2026.
[3] https://diariodarepublica.pt/dr/detalhe/decreto-lei/125-2025-962603401.
[4] https://dyn.cncs.gov.pt/pt/detalhe/art/135990/consulta-publica-projeto-de-regulamento-do-regime-juridico-da-cibersegurança.
[5] https://digital-strategy.ec.europa.eu/en/news/ict-supply-chain-security-eu-adopts-toolbox-mitigate-risks.
[6] https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act.
[7] https://www.consilium.europa.eu/en/press/press-releases/2026/03/16/cyber-attacks-against-the-eu-and-its-member-states-council-sanctions-three-entities-and-two-individuals/.

Estes atores foram sujeitos a um congelamento de bens, ficando ainda cidadãos e empresas da UE proibidos de lhes disponibilizar fundos, ativos financeiros ou recursos económicos[8]. As pessoas singulares enfrentam também uma proibição de entrar ou transitar pelo território da UE. A lista de cibersanções da UE aplica-se agora a 19 pessoas e 7 entidades. #CN #IR #ciberdiplomacia

Advogado-geral apresentou as suas conclusões ao Tribunal de Justiça da UE considerando que bancos não podem recusar o reembolso imediato de vítimas de fraude através de phishing: Num caso com origem nos tribunais polacos, o advogado-geral do Tribunal de Justiça da UE (TJUE), Athanasios Rantos, considerou, a 5 de março de 2026, que o direito da UE obriga os bancos a reembolsarem imediatamente, e numa primeira fase, o montante de uma operação não autorizada. Sem prejuízo, no entanto, que o banco possa demonstrar, numa segunda fase, que o cliente não cumpriu com as suas obrigações, nomeadamente a utilização de credenciais personalizadas, e pedir o reembolso. Estas conclusões não vinculam o TJUE, podendo os juízes decidir por uma solução jurídica diferente daquela proposta pelo advogado-geral[9]. #TJUE #phishing #banca

Autoridade de controlo de dados pessoais francesa aplicou sanções a duas operadoras de comunicações por não terem implementado medidas de segurança adequadas para proteger os dados dos seus clientes: Em outubro de 2024, um atacante obteve acesso a dados pessoais de 24 milhões de clientes de duas operadoras de comunicações eletrónicas sediadas em França. No seguimento de várias queixas, a Commission nationale de l'informatique et des libertés (CNIL) procedeu a uma ação de fiscalização onde constatou várias violações ao RGPD. Em particular, a CNIL constatou que o procedimento de autenticação para aceder à VPN das empresas e que as medidas implementadas para detetar comportamentos suspeitos nos seus sistemas de informação não eram suficientemente robustos e constituíam uma violação da obrigação de garantir a segurança dos dados pessoais nos termos do regulamento europeu[10]. #RGPD

Disrupção e Cibersabotagem[11]

Hacktivismo pró-russo cada vez mais focado em ciberataques contra sistemas OT e SCADA: Em agosto de 2025, as autoridades norueguesas atribuíram a responsabilidade de um incidente de cibersabotagem numa barragem a atores pró-russos[12]. No final do ano, a Agência federal de cibersegurança dos EUA (CISA) emitiu um aviso, em conjunto com várias congéneres de outros países, que grupos hacktivistas pró-russos estariam a explorar sistemas de acesso remoto (*virtual network computing* ou VNC) desprotegidos e expostos à Internet para obterem acesso a dispositivos de

[8] https://www.consilium.europa.eu/en/press/press-releases/2026/03/16/cyber-attacks-against-the-eu-and-its-member-states-council-sanctions-three-entities-and-two-individuals/.
[9] https://curia.europa.eu/site/upload/docs/application/pdf/2026-03/cp260031pt.pdf.
[10] https://www.cnil.fr/fr/sanction-free-2026.
[11] A informação recolhida e analisada nesta subsecção abrange o período correspondente ao quarto trimestre de 2025.
[12] https://www.theguardian.com/world/2025/aug/14/russian-hackers-control-norwegian-dam-norway; https://www.reuters.com/technology/norway-spy-chief-blames-russian-hackers-dam-sabotage-april-2025-08-13/.

controlo operacional, incluindo de entidades do setor das águas e resíduos, alimentação e agricultura, e energia[13]. #RU #intrusão #OT

Grupos hacktivistas pró-palestina apelaram à realização de ações coordenadas na efeméride dos ataques do Hamas contra Israel: Desde 7 de outubro de 2023 que grupos hacktivistas pró-palestinos apelam anualmente à participação conjunta numa campanha de ciberataques coordenados contra Israel e outros países considerados seus aliados. De acordo com o relatório da Radware[14], este apelo traduziu-se em ciberataques, de baixa complexidade e curta duração, de DDoS e modificação não autorizada de páginas de internet (*defacement*) de entidades no setor da educação, saúde, indústria transformadora, retalho e serviços financeiros. #DDoS #defacement #IL #PS

Ciberespionagem[15]

Detetada a primeira campanha de ciberespionagem conduzida substancialmente por IA generativa com intervenção humana limitada: A 13 de novembro de 2025, a Anthropic revelou ter detetado e desmantelado uma campanha de ciberespionagem em larga escala, na qual um ator estatal manipulou as ferramentas *Claude Code* e *Model Context Protocol*, assim como o modelo de linguagem em grande escala (LLM) subjacente, para desenvolver uma *pipeline* de ciberespionagem com intervenção humana mínima. Esta metodologia foi utilizada contra pelo menos 30 alvos globais, incluindo grandes empresas tecnológicas, instituições financeiras, indústria química e entidades governamentais, tendo obtido sucesso num número reduzido de casos[16]. #IA

Documentos internos revelam estrutura e *modus operandi* de unidade de ciberespionagem alinhada com o Irão: Em outubro, uma fuga de documentos internos revelou a estrutura hierárquica assim como mais detalhes do *modus operandi* do grupo APT-35, também conhecido como Charming Kitten. Os documentos revelam uma sofisticada operação interdisciplinar orientada por métricas de desempenho, assim como um crescente recurso à exploração de vulnerabilidades, nomeadamente em servidores Microsoft Exchange e ao VPN Ivanti Connect Secure, bem como a sofisticadas campanhas de *spearphishing* para obter o acesso inicial nas suas atividades de ciberespionagem[17]. #IR #APT-35

Campanha conduzida por ator estatal visa setor de veículos aéreos não tripulados na Europa: Foi identificada, em outubro de 2025, uma nova vaga da campanha *Operation DreamJob*, atribuída ao grupo norte-coreano Lazarus, na qual várias empresas europeias do setor da defesa foram visadas, incluindo entidades

[13] https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-343a.
[14] https://www.radware.com/security/threat-advisories-and-attack-reports/october-7-post-threat-analysis/.
[15] A informação recolhida e analisada nesta subsecção abrange o período correspondente ao quarto trimestre de 2025.
[16] https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf.
[17] https://dti.domaintools.com/threat-intelligence-report-apt35-internal-leak-of-hacking-campaigns-against-lebanon-kuwait-turkey-saudi-arabia-korea-and-domestic-iranian-targets/.

fortemente envolvidas no desenvolvimento de veículos aéreos não tripulados (UAV)[18]. À semelhança de outras campanhas[19], recorrem a técnicas de engenharia social baseadas em ofertas de emprego falsas para construir um pretexto para distribuir e implementar o *Remote Access Trojan* (RAT) ScoringMathTea para a exfiltração de informação. A execução do *malware* recorre a *DLL side-loading*, encriptação de *payloads* e servidores WordPress comprometidos como servidores de comando e controlo. #KP #RAT #defesa

Intensificação da campanha de *spearphishing* contra ONGs por parte de ator estatal pró-russo: Foi reportado, no último trimestre de 2025, uma intensificação das campanhas de *spearphishing* por parte do agente de ameaça Calisto (aka Coldriver, Star Blizzard), tendo como alvo duas ONGs. Nesta sofisticada campanha de engenharia social, estes atores iniciavam o seu contacto com as vítimas pedindo-lhes para reverem documentos, mas retendo deliberadamente os anexos ou enviando anexos corrompidos. Quando as vítimas solicitavam o ficheiro em falta, era-lhes enviado o *link* para uma página comprometida com redireccionadores para páginas de *phishing* que recorriam à técnica *adversary-in-the-middle*, permitindo ao adversário injetar javascript malicioso e intercetar múltiplos fatores de autenticação requisitados[20]. #RU #Spearphishing #AitM

Cibercrime[21]

Vulnerabilidades críticas em *routers* industriais exploradas para campanhas de *smishing* em massa: *Endpoints* vulneráveis de APIs de *routers* industriais utilizados para telecomunicações foram explorados por agentes de ameaça para levar a cabo campanhas de *smishing* em massa, em particular na Bélgica. Os agentes de ameaça exploraram uma vulnerabilidade crítica (EUVD-2023-47680/CVE-2023-43261), num *endpoint* da API de vários *routers* industriais da Milesight, que permitia o acesso não autenticado à funcionalidade de envio de SMS. À data do reporte, mais de 18 000 *routers* encontravam-se expostos publicamente, dos quais pelo menos 572 foram avaliados como provavelmente vulneráveis[22]. #Smishing #BE

Novo *loader-as-a-service* de origem brasileira utiliza esteganografia para ocultar *payloads* em ficheiros de imagem: Foi identificado, no último trimestre de 2025, uma nova variante de código malicioso, designada por Caminho, utilizada numa operação *loader-as-a-service*. Este código malicioso utiliza esteganografia *Least Significant Bit* para ocultar os *payloads* maliciosos em ficheiros de imagem alojados em plataformas legítimas como o archive.org. O *payload* é extraído dos dados de pixéis da imagem, carregado diretamente em memória sem escrita em disco e injetado em processos legítimos do Windows de modo a garantir a persistência. A análise do horário de atividade da operação assim como de amostras do código malicioso, que recorre

[18] https://www.welivesecurity.com/en/eset-research/gotta-fly-lazarus-targets-uav-sector/.
[19] https://www.welivesecurity.com/en/eset-research/lazarus-luring-employees-trojanized-coding-challenges-case-spanish-aerospace-company/.
[20] https://blog.sekoia.io/ngo-reporters-without-borders-targeted-by-calisto-in-recent-campaign/.
[21] A informação recolhida e analisada nesta subsecção abrange o período correspondente ao quarto trimestre de 2025.
[22] https://blog.sekoia.io/silent-smishing-the-hidden-abuse-of-cellular-router-apis/.

frequentemente ao português, sugere uma operação com origem no Brasil[23]. #LaaS #BR

Novo Trojan bancário para Android simula o comportamento humano para evitar deteção: Foi identificado um novo *trojan* bancário para Android, o Herodotus, publicitado como *malware-as-a-service*. Esta nova variante é implementada via *DLL-sideloading*, sendo o acesso inicial obtido através de um *dropper* presente em páginas de internet maliciosas distribuídas através de ataques de *smishing*. Uma vez instalado, aguarda que a vítima abra uma aplicação bancária ou de pagamentos para apresentar uma página falsa sobreposta, intercetando assim os dados bancários. Esta variante distingue-se das demais por simular de forma credível o comportamento humano ao interagir com aplicações bancárias ou de pagamentos[24]. #Trojan #banca #android

Observaram-se vários ataques à cadeia de fornecimento do ecossistema Node.js: Observaram-se, no último trimestre de 2025, várias campanhas a impactar as cadeias de fornecimento do ecossistema Node.js. Em novembro, foi detetada uma segunda vaga da campanha Shai-Hulud, um *worm* que exfiltra informação dos sistemas comprometidos e publica cópias de si mesmo no registo npm, propagando-se assim de forma autónoma pelo ecossistema[25]. Foram igualmente identificados 136 pacotes no registo npm que distribuíam *infostealers*, tendo sido descarregados cerca de 100 000 vezes[26]. Identificou-se ainda a campanha PhantomRaven, envolvendo centenas de pacotes npm, que se distingue das demais por utilizar *Remote Dynamic Dependencies* para distribuir o *payload*, tornando a sua deteção mais complexa[27]. #Cadeia-de-fornecimento #npm

Novo *kit* de *phishing-as-a-service*, Spiderman, visa dezenas de bancos europeus e plataformas de criptomoedas: Foi identificado, em dezembro de 2025, um novo *kit* de *phishing* denominado Spiderman. Este novo kit, que funciona num modelo *phishing-as-a-service*, reduz significativamente as barreiras de entrada para o cibercrime direcionado ao furto de dados financeiros, já que replica com elevada fidelidade as páginas de *login* de dezenas de bancos europeus e plataformas de criptomoedas. Esta ferramenta oferece ainda avançados mecanismos de evasão, dificultando a deteção por ferramentas de segurança automatizadas. Um grupo de Signal associado a este serviço conta com cerca de 750 membros, à data de dezembro de 2025, indicando por isso adoção ativa[28]. #PaaS #phishing

[23] https://arcticwolf.com/resources/blog/brazilian-caminho-loader-employs-lsb-steganography-to-deliver-multiple-malware-families/.
[24] https://www.threatfabric.com/blogs/new-android-malware-herodotus-mimics-human-behaviour-to-evade-detection.
[25] https://www.aikido.dev/blog/shai-hulud-strikes-again-hitting-zapier-ensdomains.
[26] https://www.securityweek.com/136-npm-packages-delivering-infostealers-downloaded-100000-times/.
[27] https://www.koi.ai/blog/phantomraven-npm-malware-hidden-in-invisible-dependencies.
[28] https://www.varonis.com/blog/spiderman-phishing-kit.

LockBit regressa com variante 5.0 e já contabiliza novas vítimas na Europa, América e Ásia: Após ter sido desmantelado pela Operação Cronos[29], foi reportado, em outubro de 2025, o regresso do *ransomware* LockBit, tendo já sido identificadas novas vítimas. A nova variante, LockBit 5.0 (pseudónimo "ChuongDong"), reforça o suporte multiplataforma assim como os mecanismos de anti análise forense, aumenta a velocidade da cifragem dos dados e introduz extensões de ficheiros aleatórias para dificultar a deteção. Os ataques abrangem a Europa Ocidental, as Américas e a Ásia, com aproximadamente 80% dirigidos a sistemas Windows e 20% a ambientes ESXi e Linux[30]. #Ransomware #lockbit

Desinformação digital e operações de informação (FIMI)[31]

Relatório dos serviços diplomáticos da UE detetou 540 incidentes relativos a operações de informações externas no último ano: Como em anos anteriores, a maior parte dos incidentes incluídos no relatório anual do Serviço Europeu de Ação Externa (EEAS) sobre *Foreign Information Manipulation and Interference Threats* tiveram a Ucrânia como alvo principal, seguido da França, Moldávia e Alemanha. Este relatório defende que uma postura puramente defensiva ou reativa dos Estados-Membros e da UE é insuficiente para fazer face a estas ameaças, sendo necessário utilizar todos os instrumentos existentes no quadro da FIMI Toolbox, incluindo sanções e partilha de informações entre entidades públicas e privadas[32]. #EEAS #FIMI #ciberdiplomacia

[29] https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation.
[30] https://blog.checkpoint.com/research/lockbit-returns-and-it-already-has-victims/.
[31] A informação recolhida e analisada nesta subsecção abrange o período correspondente ao quarto trimestre de 2025.
[32]https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf.

Vulnerabilidades Frequentemente Exploradas – T4 2025[33]

CVE/EUVD ID	CVSS v3.xx	CWEs relevantes	Data de publicação	Fabricante	Produtos afetados	Fonte
CVE-2025-64095/ EUVD-2025-36564	10	CWE-434	2025-10-29	DNNSoftware	Dnn.Platform	https://dyn.cncs.gov.pt/pt/alerta-detalhe/art/135962/alerta-de-vulnerabilidade-dnn-dotnetnuke
CVE-2025-55182	10	CWE-434	2025-12-3	Meta	React Server Components	https://euvd.enisa.europa.eu/vulnerability/CVE-2025-55182
CVE-2023-38408/ EUVD-2023-42225	9.8	N/A	2023-07-2	N/A	N/A	https://euvd.enisa.europa.eu/vulnerability/CVE-2023-38408
CVE-2025-61882/ EUVD-2025-32142	9.8	N/A	2025-10-5	Oracle Corporation	Oracle Concurrent Processing	https://euvd.enisa.europa.eu/vulnerability/CVE-2025-61882
CVE-2025-59287/ EUVD-2025-34268	9.8	N/A	2025-10-14	Microsoft	Windows Server 2012, 2012 R2, 2016, 2019, 2022, 2025	https://euvd.enisa.europa.eu/vulnerability/CVE-2025-59287
CVE-2025-49844/ EUVD-2025-33178	10	N/A	2025-10-03	Redis	Redis	https://euvd.enisa.europa.eu/vulnerability/CVE-2025-49844
CVE-2025-64446/ EUVD-2025-197613	9.4	N/A	2025-11-14	Fortinet	FortiWeb	https://euvd.enisa.europa.eu/vulnerability/CVE-2025-64446
CVE-2025-21042/ EUVD-2025-29029	8.8	CWE-787	2025-09-12	Samsung Mobile	Samsung Mobile Devices	https://euvd.enisa.europa.eu/vulnerability/CVE-2025-21042

[33] Esta lista inclui as vulnerabilidades mais exploradas no trimestre em análise segundo os dados de incidentes do CERT.PT e dados do *Vulnerability Report* do CIRCL: https://www.vulnerability-lookup.org/tags/vulnerabilityreport/.

CVE-2025-14847/ EUVD-2025-204529	8.7	N/A	2025-12-19	MongoDB Inc.	MongoDB Server	https://euvd.enisa.europa.eu/vulnerability/CVE-2025-14847
CVE-2025-20393/ EUVD-2025-203911	10	N/A	2025-12-17	Cisco	Cisco Secure Email and Web Manager	https://euvd.enisa.europa.eu/vulnerability/CVE-2025-2039

Novas Vulnerabilidades Ativamente Exploradas (KEV) - T4 2025[34]

CVE/EUVD ID	CVSS	Fabricante	Produtos afetados
CVE-2025-14847/EUVD-2025-204529	8.7 (v4.0)	MongoDB	MongoDB and MongoDB Server
CVE-2023-52163/EUVD-2023-56836	8.8 (v3.1)	Digiever	DS-2105 Pro
CVE-2025-14733/EUVD-2025-204437	9.3 (v4.0)	WatchGuard	Firebox
CVE-2025-59374/EUVD-2025-203872	9.3 (v4.0)	ASUS	Live Update
CVE-2025-40602/EUVD-2025-204255	6.6 (v3.1)	SonicWall	SMA1000 appliance
CVE-2025-20393/EUVD-2025-203911	10 (v3.1)	Cisco	Vários produtos
CVE-2025-59718/EUVD-2025-202198	9.1 (v3.1)	Fortinet	Vários produtos
CVE-2025-14611/EUVD-2025-203165	7.1 (v4.0)	Gladinet	CentreStack and Triofox
CVE-2025-43529/EUVD-2025-203963	8.8 (v3.1)	Apple	Vários produtos
CVE-2018-4063/EUVD-2018-15849	8.8 (v3.1)	Sierra Wireless	AirLink ALEOS
CVE-2025-14174/EUVD-2025-203113	8.8 (v3.1)	Google	Chromium
CVE-2025-58360/EUVD-2025-199606	8.2 (v3.1)	OSGeo	GeoServer
CVE-2025-6218/EUVD-2025-28706	7.8 (v3.0)	RARLAB	WinRAR
CVE-2025-62221/EUVD-2025-202200	7.8 (v3.1)	Microsoft	Windows
CVE-2022-37055/EUVD-2022-39709	9.8 (v3.1)	D-Link	Routers

[34] Esta lista inclui uma seleção de Vulnerabilidades Ativamente Exploradas identificadas e publicadas este trimestre pela CISA no seu catálogo Known Exploited Vulnerability (KEV). Para aceder ao catálogo completo: https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

CVE-2025-66644/EUVD-2025-201500	7.2 (v3.1)	Array Networks	ArrayOS AG
CVE-2025-55182/EUVD-2025-200983	10 (v3.1)	Meta	React Server Components
CVE-2021-26828/EUVD-2021-13613	8.8 (v3.1)	OpenPLC	ScadaBR
CVE-2025-48633/EUVD-2025-201737	5.5 (v3.1)	Android	Framework
CVE-2025-48572/EUVD-2025-201776	7.8 (v3.1)	Android	Framework
CVE-2025-61757/EUVD-2025-35253	9.8 (v3.1)	Oracle	Fusion Middleware
CVE-2025-13223/EUVD-2025-197896	8.8 (v3.1)	Google	Chromium V8
CVE-2025-58034/EUVD-2025-198020	6.7 (v3.1)	Fortinet	FortiWeb
CVE-2025-64446/EUVD-2025-197613	9.4 (v3.1)	Fortinet	FortiWeb
CVE-2025-12480/EUVD-2025-44062	9.1 (v3.1)	Gladinet	Triofox
CVE-2025-62215/EUVD-2025-93397	7 (v3.1)	Microsoft	Windows
CVE-2025-21042/EUVD-2025-29029	8.8 (v3.1)	Samsung	Mobile Devices
CVE-2025-48703/EUVD-2025-30324	9 (v3.1)	CWP	Control Web Panel
CVE-2025-11371/EUVD-2025-33408	7.5 (v3.1)	Gladinet	CentreStack and Triofox
CVE-2025-41244/EUVD-2025-31589	7.8 (v3.1)	Broadcom	VMware Aria Operations and VMware Tools
CVE-2025-24893/EUVD-2025-4562	9.8 (v3.1)	XWiki	Platform
CVE-2025-6204/EUVD-2025-23494	8 (v3.1)	Dassault Systemes	DELMIA Apriso
CVE-2025-6205/EUVD-2025-23493	9.1 (v3.1)	Dassault Systemes	DELMIA Apriso
CVE-2025-54236/EUVD-2025-27277	9.1 (v3.1)	Adobe	Commerce and Magento
CVE-2025-59287/EUVD-2025-34268	9.8 (v3.1)	Microsoft	Windows

CVE-2025-61932/EUVD-2025-35038	9.3 (v4.0)	Motex	LANSCOPE Endpoint Manager
CVE-2022-48503/EUVD-2022-51199	8.8 (v3.1)	Apple	Vários produtos
CVE-2025-2746/EUVD-2025-8008	9.8 (v3.1)	Kentico	Xperience CMS
CVE-2025-2747/EUVD-2025-8009	9.8 (v3.1)	Kentico	Xperience CMS
CVE-2025-33073/EUVD-2025-17737	8.8 (v3.1)	Microsoft	Windows
CVE-2025-61884/EUVD-2025-33878	7.5 (v3.1)	Oracle	E-Business Suite
CVE-2025-54253/EUVD-2025-23647	10 (v3.1)	Adobe	Experience Manager (AEM) Forms
CVE-2025-47827/EUVD-2025-16999	4.6 (v3.1)	IGEL	IGEL OS
CVE-2025-24990/EUVD-2025-34257	7.8 (v3.1)	Microsoft	Windows
CVE-2025-59230/EUVD-2025-34258	7.8 (v3.1)	Microsoft	Windows
CVE-2016-7836/EUVD-2016-8685	9.8 (v3.1)	SKYSEA	Client View
CVE-2021-43798/EUVD-2024-0581	7.5 (v3.1)	Grafana	Labs Grafana
CVE-2025-27915/EUVD-2025-7823	5.4 (v3.1)	Synacor	Zimbra Collaboration Suite (ZCS)
CVE-2021-22555/EUVD-2021-9696	8.3 (v3.1)	Linux	Kernel
CVE-2010-3962/EUVD-2010-3939	8.1 (v3.1)	Microsoft	Internet Explorer
CVE-2021-43226/EUVD-2021-30170	7.8 (v3.1)	Microsoft	Windows
CVE-2013-3918/EUVD-2013-3850	8.8 (v3.1)	Microsoft	Windows
CVE-2025-61882/EUVD-2025-32142	9.8 (v3.1)	Oracle	E-Business Suite
CVE-2014-6278/EUVD-2014-6163	8.8 (v3.1)	GNU	GNU Bash
CVE-2017-1000353/EUVD-2022-1921	9.8 (v3.1)	Jenkins	Jenkins

CVE-2015-7755/EUVD-2015-7655	9.8 (v3.1)	Juniper	ScreenOS
CVE-2025-21043/EUVD-2025-29028	8.8 (v3.1)	Samsung	Mobile Devices
CVE-2025-4008/EUVD-2025-16032	8.7 (v4.0)	Smartbedded	Meteobridge