CNCS Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança

TLP:CLEAR

30 de junho de 2026

Boletim do Observatório de Cibersegurança do CNCS

N.º 2/2026

Destaques[1]

- Com a publicação do Regulamento n.º 756/2026 começam a contar vários prazos legais para as entidades públicas e privadas que se encontrem no âmbito do Regime Jurídico da Cibersegurança em Portugal; a Comissão Europeia procura reforçar a "**soberania tecnológica europeia**", ao mesmo tempo que o governo dos EUA proibiu temporariamente o acesso de estrangeiros aos modelos mais avançados de IA da Anthropic.

- Diversas entidades prestadoras de serviços nos setores da energia e tratamento de águas na Polónia foram alvo de **atos e tentativas de cibersabotagem** no último ano; ataque de DDoS a empresa estatal ferroviária alemã com elevado impacto operacional; grupo hacktivista associado ao Irão reivindica ataque contra empresa de tecnologia médica norte-americana estabelecida na Irlanda.

- Vulnerabilidade crítica no WinRaR **continua a ser explorada ativamente**, apesar da existência de uma correção desde julho 2025; foi identificada uma campanha de **ciberespionagem** atribuída ao grupo APT28 (*Fancy Bear*) que explora uma vulnerabilidade no Microsoft Office; este mesmo grupo expôs inadvertidamente a sua infraestrutura revelando métodos e alvos das suas operações.

- Falsos *Blue Screen of Death* utilizados em novas campanhas de distribuição de *malware* com recurso à técnica de engenharia social *ClickFix*; foi detetado reaparecimento do **LummaStealer**; foi também identificada uma lista compilada com 45 milhões de dados de cidadãos franceses expostos na internet; ciberataque a uma agência governamental francesa expôs ainda dados relativos a 11.7 milhões de contas.

[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]

Foi publicado o Regulamento de execução do Regime Jurídico da Cibersegurança e disponibilizada a plataforma MyCiber: Com a publicação do Regulamento[3] inicia a contagem do prazo legal de 24 meses para a produção de efeitos das medidas de cibersegurança e da obrigatoriedade de comunicação do relatório Anual pelas entidades essenciais. As entidades têm a obrigação de identificação e registo na Plataforma MyCiber[4], podendo comunicar, nesta primeira fase, com as autoridades de cibersegurança competentes: CNCS, Autoridade Nacional de Comunicações (ANACOM) e Gabinete Nacional de Segurança (GNS)[5]. #NIS2

Comissão apresenta pacote legislativo e políticas de reforço da "soberania tecnológica europeia": De acordo com o relatório Draghi, a UE depende estruturalmente de fornecedores de países externos à UE para mais de 80 % dos seus produtos, serviços, infraestruturas e propriedade intelectual digitais[6]. Em junho deste ano, quase dois anos após a publicação deste relatório, a Comissão apresentou um pacote composto por quatro iniciativas, incluindo uma atualização do regulamento que enquadra o desenvolvimento e comercialização de semicondutores, conhecido por Chips Act, com o fim de reforçar a produção europeia deste produto; uma proposta de regulamento para enquadrar o ecossistema europeu das tecnologias *cloud* e inteligência artificial, conhecido por CADA (*Cloud and AI Development Act*), que prevê a classificação de fornecedores de serviços *cloud* em função do seu nível de dependência externa; uma estratégia que aposta no *software open source* como uma alternativa europeia às soluções proprietárias de países terceiros garantindo apoio financeiro; e um plano de ação para a digitalização e inteligência artificial no setor da energia[7]. #Soberaniadigital

Relatório da ENISA identifica oito setores críticos com baixos níveis de maturidade em cibersegurança a nível da UE: Os setores da saúde, transportes ferroviários e marítimos, os serviços de gestão de TIC, setor espacial, administração publica e o abastecimento de água potável e tratamento de águas residuais encontram-se na "zona de risco" do último Relatório 360ª da Agência europeia de cibersegurança (ENISA). O conceito de "zona de risco" inclui setores com um nível de maturidade em cibersegurança inferior à média e cuja criticidade excede a sua maturidade. Os setores críticos com maior nível de maturidade são: banca, eletricidade e telecomunicações, tendo se registado avanços particularmente importantes a nível da maturidade no setor do gás[8]. #NIS2 #Saude #Transportes #Energia #Aguas #AP #Espaco

Países Baixos impedem a aquisição de empresa prestadora de serviços *cloud* pela empresa americana Kyndryl: O governo dos Países Baixos bloqueou, no

[2] A informação recolhida e analisada nesta subsecção abrange o período correspondente ao segundo trimestre de 2026.
[3] https://dyn.cncs.gov.pt/pt/detalhe/art/136022/regulamento-do-regime-juridico-da-ciberseguranca-publicado.
[4] https://myciber.gov.pt/.
[5] https://diariodarepublica.pt/dr/detalhe/regulamento/756-2026-1134399056.
[6] https://commission.europa.eu/topics/competitiveness/draghi-report_en#paragraph_47059.
[7] https://digital-strategy.ec.europa.eu/en/library/communication-european-tech-sovereignty-accompanied-eu-open-source-strategy.
[8] https://www.enisa.europa.eu/enisa-nis360-2026.

dia 25 de maio, a venda da empresa Solvinity, que gere a plataforma de alojamento DigiD, utilizada como portal seguro para aceder a registos confidenciais e comunicar com a administração fiscal, segurança social, saúde e autarquias locais[9]. Apesar do regulador da concorrência ter dado luz verde ao negócio, este acabou por ser vetado pelo ministro responsável pela economia digital e soberania por razões de "interesse público" após a realização de uma avaliação no âmbito da Lei relativa ao controlo indesejável nas telecomunicações (WOZT) no que diz respeito à avaliação no setor das infraestruturas digitais[10]. #NIS2 #soberaniadigital

EUA ordena a suspensão do acesso de cidadãos estrangeiros aos últimos modelos de IA da Anthropic por razões de segurança nacional: Após receber esta ordem por parte do Departamento do Comércio do Governo Federal dos EUA, no dia 12 de junho, a empresa norte-americana suspendeu o acesso de qualquer cidadão estrangeiro, incluindo aqueles residentes nos EUA e trabalhadores da empresa, aos modelos Fable 5 e Mythos 5[11]. Esta proibição surge poucas semanas depois da empresa ter garantido o acesso das autoridades europeias ao Mythos, um modelo com capacidades avançadas de deteção e exploração de vulnerabilidades, após várias semanas de espera e negociação[12]. De acordo com um estudo da AI Security Institute (AISI), as capacidades dos últimos modelos de IA (p. ex. Mythos, GPT-5.5) têm vindo a duplicar, observando-se uma aceleração que ultrapassa as melhores previsões[13]. #IA #soberaniadigital

Disrupção e Cibersabotagem[14]

Polónia trava tentativa de cibersabotagem contra a sua rede elétrica, mas não evita ataques contra sistemas de controlo do tratamento de água: As autoridades polacas divulgaram que, no final de dezembro de 2025, foi detetada e neutralizada uma operação de cibersabotagem dirigida à infraestrutura elétrica nacional, com vista a comprometer as comunicações entre instalações de energias renováveis e operadores de distribuição. O incidente, descrito como um dos mais graves dos últimos anos, esteve perto de causar um apagão em larga escala, segundo fontes governamentais, tendo afetado múltiplas fontes de produção de energias renováveis, como parques eólicos e solares. Mais recentemente, os serviços de informações polacos confirmaram que foram atacadas estações de controlo de tratamento de água de cinco localidades, tendo em alguns casos os atacantes acedido aos sistemas de controlo industrial[15]. Estes casos reflete uma evolução nas táticas de ataque a infraestruturas críticas, com enfoque em sistemas energéticos distribuídos e interdependentes, e evidencia a crescente exposição destes setores a ameaças de natureza geopolítica[16]. #Energia #Agua #OT

[9] https://www.dutchnews.nl/2026/05/dutch-government-blocks-sale-of-digid-owner-to-us-tech-giant/.
[10] https://open.overheid.nl/details/ec64d1c2-381a-43c3-9b15-06ba3399fb67.
[11] https://www.anthropic.com/news/fable-mythos-access.
[12] https://www.politico.eu/article/anthropic-invites-eu-to-access-mythos-hacking-tech/.
[13] https://www.aisi.gov.uk/blog/how-fast-is-autonomous-ai-cyber-capability-advancing.
[14] A informação recolhida e analisada nesta subsecção abrange o período correspondente ao segundo trimestre de 2026.
[15] https://therecord.media/polish-intelligence-warns-hackers-attacked-water-treatment.
[16] https://therecord.media/poland-cyberattack-grid-russia.

A empresa estatal de transportes ferroviários alemã foi alvo de um ataque DDoS com impacto operacional: Em fevereiro de 2026, a Deutsche Bahn foi alvo de um ciberataque do tipo negação de serviço distribuída (DDoS) que comprometeu temporariamente o funcionamento das suas plataformas digitais, incluindo os sistemas de venda de bilhetes e de consulta de horários[17]. De acordo com o relatório ENISA Threat Landscape 2025, o setor dos transportes foi o segundo mais visado por grupos hacktivistas durante 2025, representando cerca de 12% de todos os incidentes atribuídos a estes grupos, evidenciando a crescente exposição deste setor à cibersabotagem e outros ataques disruptivos[18]. #DDoS #DE #Transportes

Grupo hacktivista associado ao Irão reivindica ataque que apagou dados de uma empresa de tecnologia médica na Irlanda: A Stryker, empresa norte americana de tecnologia médica, reportou, em março de 2026, um ciberataque que comprometeu os seus sistemas informáticos, provocando a interrupção das operações a nível global. O incidente, de natureza altamente disruptiva, envolveu o recurso a um *wiper* para a eliminação massiva de dados em sistemas e dispositivos associados à rede da empresa. O ataque foi reivindicado pelo grupo Handala (também conhecido por Handala Hack Team), que se apresenta como um coletivo hacktivista pró-palestina, mas cuja atividade se encontra frequentemente alinhada com objetivos estratégicos e operacionais iranianos, sendo por isso recorrentemente atribuído a esse ator estatal[19]. Este ataque surge no contexto do conflito no Irão, enquadrando-se, por isso, numa intensificação das atividades no ciberespaço por parte de atores ligados a este país. #IR #Wiper

Ciberespionagem[20]

Exploração generalizada de vulnerabilidade crítica no WinRaR por múltiplos atores maliciosos: Foi identificada a exploração ativa e generalizada da vulnerabilidade CVE-2025-8088 no WinRar, uma popular ferramenta de compressão de ficheiros em sistemas Windows. Esta vulnerabilidade permite a execução de ataques do tipo *path traversal* e a sua exploração ocorre tipicamente através de ficheiros RaR manipulados que combinam conteúdos legítimos com *payloads* ocultos. Apesar de ter sido corrigida em julho de 2025, esta vulnerabilidade, classificada como crítica, continua a ser explorada como vetor de acesso inicial por diversos atores, incluindo grupos associados a atores estatais e cibercriminosos como os Initial Acess Brokers[21]. #WinRaR #CVE-2025-8088

Ator estatal explora vulnerabilidade no Microsoft Office 24 horas após a sua divulgação em campanha de ciberespionagem: Foi identificada uma campanha de ciberespionagem atribuída ao grupo APT28 (também conhecido por *Fancy Bear*), que explora ativamente a vulnerabilidade CVE 2026-21509 no Microsoft Office, um dia após a sua divulgação pública, para obter acesso inicial a sistemas de entidades

[17] https://www.dw.com/en/deutsche-bahn-says-cyberattack-hit-ticket-and-info-systems/a-76024130.
[18] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.
[19] https://www.justice.gov/opa/pr/justice-department-disrupts-iranian-cyber-enabled-psychological-operations.
[20] A informação recolhida e analisada nesta subsecção abrange o período correspondente ao quarto trimestre de 2025.
[21] https://cloud.google.com/blog/topics/threat-intelligence/exploiting-critical-winrar-vulnerability.

governamentais e militares, em particular na Europa. A exploração ocorre através de campanhas de *spearphishing* com documentos maliciosos que executam código automaticamente aquando da sua abertura, sem necessidade de interação adicional. Esta campanha de *spearphishing* visou sobretudo ministérios da defesa, operadores de transportes e logística assim como entidades diplomáticas, utilizando para o efeito como "isco" mensagens que exploram narrativas geopolíticas como consultas diplomáticas no âmbito da NATO ou convites para programas militares[22]. #APT28 #CVE-2026-21509

Infraestrutura acidentalmente exposta revela métodos e alvos das operações de ciberespionagem do grupo APT28: Parte da infraestrutura de comando e controlo do grupo APT28 (também conhecido por *Fancy Bear*) ficou exposta a utilizadores externos devido a falhas de segurança operacional, permitindo o acesso, por parte de investigadores, a dados sensíveis associados às suas operações, incluindo milhares de emails, credenciais e contactos de vítimas. Esta exposição veio corroborar tendências previamente identificadas com base em fontes abertas, nomeadamente o foco em entidades governamentais e militares na Europa, com particular incidência em países alinhados com a NATO e no apoio à Ucrânia, recorrendo sobretudo a campanhas de *spearphishing* altamente direcionadas. A análise da infraestrutura exposta permitiu ainda identificar um conjunto consistente de técnicas utilizadas pelo grupo, incluindo a exploração de vulnerabilidades *cross-site scripting* em clientes de *webmail* para injeção de código malicioso e exfiltração de informação, bem como mecanismos de persistência, nomeadamente através da criação de regras de reencaminhamento automático de *emails*, permitindo o acesso contínuo às comunicações das vítimas sem necessidade de nova intrusão[23]. #APT28 # opsec

Cadeia de ataque iOS que explora múltiplos *zero-days* utilizada por atores estatais e privados: Investigadores do Google Threat Intelligence Group identificaram o DarkSword, uma cadeia de exploração (*exploit chain*) para iOS que utiliza múltiplas vulnerabilidades *zero-day* para comprometer dispositivos, tendo sido observada a sua utilização por diversos atores, incluindo fornecedores privados de serviços de ciberespionagem (*private sector offensive actor*) assim como grupos associados a Estados, desde pelo menos novembro de 2025. A cadeia de infeção é composta por múltiplas etapas, iniciando-se tipicamente através de *websites* maliciosos que exploram vulnerabilidades no *browser* do iOS para obter execução remota de código, seguida de técnicas de evasão, *sandbox escape* e elevação de privilégios, culminando na instalação de *payloads* de *spyware*. A utilização simultânea do DarkSword por diversos atores, em diferentes geografias e movidos por diferentes motivações, demonstram o impacto generalizado da indústria do *spyware*.[24]. #iOS #zero-day

[22] https://www.trellix.com/blogs/research/apt28-stealthy-campaign-leveraging-cve-2026-21509-cloud-c2/.
[23] https://ctrlaltintel.com/research/FancyBear/.
[24] https://cloud.google.com/blog/topics/threat-intelligence/darksword-ios-exploit-chain.

Cibercrime[25]

Operação internacional conjunta desmantela infraestrutura utilizada para realizar ataques de DDoS com mais de 75 000 utilizadores: No dia 13 de abril, a EUROPOL e forças de segurança nacionais de 21 países, incluindo Portugal, apreenderam 53 domínios que alojavam serviços de DDoS a soldo (*DDoS-for-hire*). Foram detidos quatros suspeitos na sequência de 25 buscas domiciliárias, tendo ainda sido enviadas cartas e *emails* a mais de 75 000 utilizadores inscritos nestes serviços ilegais. Este tipo de infraestrutura, composta por servidores, bases de dados e outros componentes, permite que pessoas com poucos conhecimentos técnicos sigam instruções, passo a passo, para executarem ataques criminosos. Os ataques de DDoS causam prejuízos significativos a empresas e particulares, visando servidores, páginas de internet ou serviços *online* tornando-os inacessíveis aos utilizadores[26]. #DDoS #EUROPOL

Falsos *Blue Screen of Death* (BSOD) utilizados em novas campanhas de distribuição de *malware* com recurso à técnica de engenharia social *ClickFix*: Foi identificada uma campanha de distribuição de *malware* que utiliza a técnica de engenharia social *ClickFix*, iniciando-se com *emails* de *phishing* que imitam notificações de cancelamento de reservas associadas a uma conhecida plataforma de reserva de alojamento de modo a direcionar as vítimas para páginas maliciosas. Nestas páginas, os atacantes recorrem a mecanismos de manipulação do utilizador, nomeadamente através da apresentação de um falso erro em formato semelhante a um CAPTCHA. Ao interagir com este elemento, a vítima desencadeia uma simulação de *Blue Screen of Death* (BSOD), integralmente gerada em HTML, não correspondendo a qualquer falha real do sistema. Esta simulação cria um contexto de urgência e perceção de erro crítico, levando o utilizador a seguir instruções apresentadas no ecrã. Estas instruções consistem numa sequência de ações aparentemente benignas, que resultam na execução manual de código malicioso pelo próprio utilizador[27]. #Engenharia-social #ClickFix

Mais de 45 milhões de dados de cidadãos franceses expostos em base de dados associada a atividades cibercriminosas: Foi identificada uma base de dados acessível publicamente com mais de 45 milhões de dados pessoais de cidadãos franceses. O repositório, encontrado num servidor localizado em França, incluía dados de diversos tipos, como dados demográficos, informação de saúde, dados financeiros e informação relacionada com veículos e seguros. A análise sugere que a base de dados terá sido compilada por atores maliciosos, como *data brokers* ilícitos, com o objetivo de consolidar diferentes conjuntos de dados numa única fonte, aumentando o seu valor e permitindo a correlação de identidades. Este tipo de agregação possibilita a construção de perfis detalhados das vítimas, facilitando a realização de fraudes, roubo de identidade

[25] A informação recolhida e analisada nesta subsecção abrange o período correspondente ao primeiro trimestre de 2026.
[26] https://www.europol.europa.eu/media-press/newsroom/news/europol-supported-global-operation-targets-over-75-000-users-engaged-in-ddos-attacks.
[27] https://www.securonix.com/blog/analyzing-phaltblyx-how-fake-bsods-and-trusted-build-tools-are-used-to-construct-a-malware-infection/.

e campanhas de engenharia social altamente direcionadas[28]. #Violação-de-dados-pessoais #FR

Ciberataque a agência governamental francesa expõe dados relativos a 11.7 milhões de contas: O organismo público responsável pelos documentos de identidade, incluindo cartões de identidades, passaportes, autorizações de residência e cartas de condução, a *Agence nationale des titres sécurisés* (ANTS), também conhecida como *France Titres*, foi afetado por um incidente de cibersegurança detetado a 15 de abril[29]. De acordo com o Ministério da Administração Interna francês os dados expostos incluem as credenciais de acesso, nome, endereços eletrónicos, data de nascimento, mas também, em alguns casos, o endereço postal e número de telefone. Estima-se que o ataque tenha sido levado a cabo por um jovem sem conhecimentos técnicos avançados (*script kiddie*) que se limitou a explorar um erro de configuração que permitiu a manipulação do URL da página da agência permitindo, posteriormente, o acesso indevido a contas de terceiros[30]. #Violação-de-dados-pessoais #FR

Reaparecimento do LummaStealer marca nova vaga de ataques após disrupção em 2025: Foi detetado um reaparecimento do *infostealer* Lumma (também conhecido por LummaStealer), menos de um ano após a sua disrupção parcial fruto de uma operação policial internacional[31]. As campanhas recentes baseiam-se predominantemente em técnicas de engenharia social, destacando-se o recurso à técnica ClickFix. A distribuição desta variante suportada pelo *loader* CastleLoader, que executa *payloads* em memória recorrendo a avançados mecanismos de evasão. Cumpre relembrar que, tal com discutido no Relatório Anual de Segurança Interna 2025, os *infostealers* representaram 94% de todas as variantes detetadas pelo CERT.PT em 2025, sendo a variante Lumma a mais frequentemente observada[32]. #LummaStealer #infostealer

Comprometimento da ferramenta de segurança Trivy desencadeia ataque às cadeias de fornecimento de várias organizações incluindo a Comissão Europeia: A 19 de março de 2026, o ator TeamPCP publicou versões maliciosas do Trivy, uma ferramenta *open source* de análise de vulnerabilidades amplamente utilizada em pipelines CI/CD. O ataque teve origem na exploração de uma configuração incorreta no ambiente de desenvolvimento da plataforma de controlo de versões (nomeadamente, no GitHub Actions) do projeto, que permitiu a extração de um *token* de acesso privilegiado. O atacante usou esse acesso para alterar "tags" de versões da ferramenta de modo a apontá-las para código malicioso (*tag poisoning*). Assim quem referenciava essas *tags* acabava por executar o código malicioso ao invés das versões legítimas da ferramenta. Este código malicioso roubava segredos de ambientes de desenvolvimento, como por exemplo credenciais *cloud*, chaves SSH ou *tokens* Kubernetes, exfiltrando-os

[28] https://cybernews.com/security/millions-french-citizen-records-leaked/.
[29] https://www.lemonde.fr/societe/article/2026/04/22/la-fuite-de-donnees-a-l-agence-nationale-des-titres-securises-nouvelle-illustration-des-failles-de-securite-des-services-informatiques-de-l-etat_6682449_3224.html.
[30] https://www.bfmtv.com/tech/actualites/cybersecurite/ants-comment-une-simple-erreur-de-configuration-a-permis-a-un-jeune-homme-de-19-ans-sans-connaissance-technique-avancee-de-pirater-les-donnees-de-pres-de-12-millions-de-personnes_AV-202606160869.html.
[31] https://www.bitdefender.com/en-us/blog/labs/lummastealer-second-life-castleloader.
[32] https://portugal.gov.pt/gc25/comunicacao/documentos/rasi-2025-relatorio-anual-de-seguranca-interna.

para infraestrutura controlada pelo atacante[33]. O CERT-EU confirmou, com elevada confiança, que este comprometimento constituiu o vetor de acesso inicial à infraestrutura AWS da Comissão Europeia, tendo o ator exfiltrado vários GB de dados comprimidos relativos a *websites* alojados de várias unidades da Comissão e outras entidades da UE. Os dados, que incluem nomes, endereços de *email* e conteúdo de comunicações, foram publicados pelo grupo de extorsão ShinyHunters a 28 de março[34]. #Cadeia-de-fornecimento #Comissão-Europeia

Desinformação digital e operações de informação (FIMI)[35]

Rede global de burlas de investimento recorre a anúncios e páginas de desinformação para enganar vítimas: Investigadores identificaram uma infraestrutura global de burlas de investimento que recorre a anúncios pagos em redes sociais, com conteúdo em mais de 15 línguas e narrativas fabricadas envolvendo figuras públicas e meios de comunicação social reais para direcionar vítimas para esquemas fraudulentos de investimento. As campanhas utilizavam táticas típicas de campanhas de desinformação e de engenharia social como a clonagem de páginas de meios de comunicação e recurso ao *typosquatting*. Recorriam também a narrativas fabricadas, nomeadamente escândalos relacionados com o setor financeiro, falsos testamentos de celebridades e falsas investigações a políticos, adaptados a cada país. Esta campanha envolveu mais de 26 000 anúncios e foi observada em pelo menos 25 países, incluindo Portugal [36]. #Burla #Desinformação

[33] https://www.aquasec.com/blog/trivy-supply-chain-attack-what-you-need-to-know/.
[34] https://cert.europa.eu/blog/european-commission-cloud-breach-trivy-supply-chain.
[35] A informação recolhida e analisada nesta subsecção abrange o período correspondente ao primeiro trimestre de 2026.
[36] https://www.bitdefender.com/en-us/blog/labs/global-investment-scam-network-using-meta-ads.

Vulnerabilidades Frequentemente Exploradas – T1 2026[37]

CVE/EUVD ID	CVSS	CWEs relevantes	Data de publicação	Fabricante	Produtos afetados	Fonte
CVE-2025-14500/EUVD-2025-205006	9.8	CWE-78	2025-12-11	IceWarp	IceWarp	https://dyn.cncs.gov.pt/pt/alerta-detalhe/art/135988/alerta-de-vulnerabilidade-icewarp
CVE-2026-1731/EUVD-2026-5559	9.9	CWE-78	2026-02-06	BeyondTrust	Remote Support(RS) & Privileged Remote Access(PRA)	https://euvd.enisa.europa.eu/vulnerability/CVE-2026-1731
CVE-2025-54068/EUVD-2025-21792	9.2	CWE-94	2025-07-17	Livewire	Livewire	https://dyn.cncs.gov.pt/pt/alerta-detalhe/art/135992/alerta-de-vulnerabilidade-livewire
CVE-2026-20963/EUVD-2026-2114	9.8	CWE-502	2026-1-13	Microsoft	Microsoft SharePoint Enterprise Server 2016, Microsoft SharePoint Server 2019, Microsoft SharePoint Server Subscription Edition	https://dyn.cncs.gov.pt/pt/alerta-detalhe/art/135993/alerta-de-vulnerabilidade-microsoft-office-sharepoint
CVE-2025-53521/EUVD-2025-34630	9.3	CWE-121	2025-10-15	F5	BIG-IP	https://dyn.cncs.gov.pt/pt/alerta-detalhe/art/135995/alerta-de-vulnerabilidade-f5-big-ip-apm
CVE-2026-20131/EUVD-2026-9444	10	CWE-502	2026-03-04	Cisco	Cisco Secure Firewall Management Center (FMC)	https://dyn.cncs.gov.pt/pt/alerta-detalhe/art/135996/alerta-de-vulnerabilidade-cisco-secure-fmc
CVE-2026-3055/EUVD-2026-14546	9.3	CWE-125	2026-03-23	Citrix	NetScaler ADC e Gateway	https://euvd.enisa.europa.eu/vulnerability/CVE-2026-3055
CVE-2026-2441/EUVD-	8.8	CWE-416	2026-02-13	Google	Chrome	https://euvd.enisa.europa.eu/vulnerability/CVE-2026-2441

[37] 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/.

2026-6071						
CVE-2026-21858/ EUVD-2026-1187	10	CWE-20	2026-01-07	n8n-io	n8n	https://euvd.enisa.europa.eu/vulnerability/CVE-2026-21858
CVE-2026-24061/ EUVD-2026-3688	9.8	CWE-88	2026-01-21	GNU	Inetutils	https://euvd.enisa.europa.eu/vulnerability/CVE-2026-24061

Novas Vulnerabilidades Ativamente Exploradas (KEV) – T1 2026[38]

CVE/EUVD ID	CVSS	Fabricante	Produtos afetados
CVE-2026-3055/EUVD-2026-14546	9.3	Citrix	NetScaler
CVE-2025-53521/EUVD-2025-34630	9.3	F5	BIG-IP
CVE-2026-33634/EUVD-2026-14601	9.4	Aquasecurity	Trivy
CVE-2026-33017/EUVD-2026-13556	9.3	Langflow	Langflow
CVE-2025-32432/EUVD-2025-12521	10	Craft CMS	Craft CMS
CVE-2025-54068/EUVD-2025-21792	9.2	Laravel	Livewire
CVE-2025-43510/EUVD-2025-203138	7.8	Apple	Vários produtos
CVE-2025-43520/EUVD-2025-203153	5.5	Apple	Vários produtos
CVE-2025-31277/EUVD-2025-23063	8.8	Apple	Vários produtos
CVE-2026-20131/EUVD-2026-9444	10	Cisco	Secure Firewall Management Center (FMC)
CVE-2025-66376/EUVD-2026-0850	7.2	Synacor	Zimbra Collaboration Suite (ZCS)
CVE-2026-20963/EUVD-2026-2114	9.8	Microsoft	SharePoint
CVE-2025-47813/EUVD-2025-21020	4.3	Wing FTP Server	Wing FTP Server
CVE-2026-3910/EUVD-2026-11736	8.8	Google	Chromium V8
CVE-2026-3909/EUVD-2026-11734	8.8	Google	Skia

[38] 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-2025-68613/EUVD-2025-204618	10	n8n	n8n
CVE-2021-22054/EUVD-2021-9219	7.5	Omnissa	Workspace One UEM
CVE-2025-26399/EUVD-2025-30842	9.8	SolarWinds	Web Help Desk
CVE-2026-1603/EUVD-2026-6842	8.6	Ivanti	Endpoint Manager (EPM)
CVE-2017-7921/EUVD-2017-16892	9.8	Hikvision	Vários produtos
CVE-2021-22681/EUVD-2021-9817	9.8	Rockwell	Vários produtos
CVE-2023-43000/EUVD-2023-47421	8.8	Apple	Vários produtos
CVE-2021-30952/EUVD-2021-17869	8.8	Apple	Vários produtos
CVE-2023-41974/EUVD-2023-46433	7.8	Apple	iOS and iPadOS
CVE-2026-22719/EUVD-2026-8708	8.1	Broadcom	VMware Aria Operations
CVE-2026-21385/EUVD-2026-9202	7.8	Qualcomm	Multiple Chipsets
CVE-2022-20775/EUVD-2022-26025	7.8	Cisco	SD-WAN
CVE-2026-20127/EUVD-2026-8675	10	Cisco	Catalyst SD-WAN Controller and Manager
CVE-2026-25108/EUVD-2026-6172	8.8	Soliton Systems K.K	FileZen
CVE-2025-49113/EUVD-2025-16605	9.9	Roundcube	Webmail
CVE-2025-68461/EUVD-2025-204035	7.2	Roundcube	Webmail
CVE-2021-22175/EUVD-2021-9321	6.8	GitLab	GitLab
CVE-2026-22769/EUVD-2026-7966	10	Dell	RecoverPoint for Virtual Machines (RP4VMs)
CVE-2020-7796/EUVD-2020-28728	9.8	Synacor	Zimbra Collaboration Suite
CVE-2024-7694/EUVD-2024-48579	7.2	TeamT5	ThreatSonar Anti-Ransomware

CVE-2008-0015/EUVD-2008-0028	8.8	Microsoft	Windows
CVE-2026-2441/EUVD-2026-6071	8.8	Google	Chromium
CVE-2026-1731/EUVD-2026-5559	9.9	BeyondTrust	Remote Support (RS) and Privileged Remote Access (PRA)
CVE-2026-20700/EUVD-2026-6189	7.8	Apple	Multiple Products
CVE-2024-43468/EUVD-2024-40737	9.8	Microsoft	Configuration Manager
CVE-2025-15556/EUVD-2025-206661	7.7	Notepad++	Notepad++
CVE-2025-40536/EUVD-2025-206418	8.1	SolarWinds	Web Help Desk
CVE-2026-21513/EUVD-2026-7342	8.8	Microsoft	Windows
CVE-2026-21525/EUVD-2026-7329	6.2	Microsoft	Windows
CVE-2026-21510/EUVD-2026-7337	8.8	Microsoft	Windows
CVE-2026-21533/EUVD-2026-7343	7.8	Microsoft	Windows
CVE-2026-21519/EUVD-2026-7358	7.8	Microsoft	Windows
CVE-2026-21514/EUVD-2026-7334	7.8	Microsoft	Office
CVE-2025-11953/EUVD-2025-37505	9.8	React Native Community	CLI
CVE-2026-24423/EUVD-2026-4273	9.3	SmarterTools	SmarterMail
CVE-2021-39935/EUVD-2021-26291	6.8	GitLab	Community and Enterprise Editions
CVE-2025-64328/EUVD-2025-38232	8.6	Sangoma	FreePBX
CVE-2019-19006/EUVD-2019-8659	9.8	Sangoma	FreePBX
CVE-2025-40551/EUVD-2025-206426	9.8	SolarWinds	Web Help Desk
CVE-2026-1281/EUVD-2026-4940	9.8	Ivanti	Endpoint Manager Mobile (EPMM)

CVE-2026-24858/EUVD-2026-4712	9.4	Fortinet	Vários produtos
CVE-2018-14634/EUVD-2018-6537	7.8	Linux	Kernel
CVE-2025-52691/EUVD-2025-205544	10	SmarterTools	SmarterMail