wavecom

Connecting every...things

Soluções criativas e inovadoras na área de engenharia de comunicações.

Política de Divulgação Coordenada de Vulnerabilidades

September 2026

Índice

1. Controlo do Documento

> *UE 2024/2847 (CRA) — Art. 13.º(8): os fabricantes têm de dispor de políticas e procedimentos para o tratamento de vulnerabilidades. Tem de existir um documento de política, versionado, com dono atribuído e revisto regularmente.*

Campo	Wavecom
Nome da Organização	WAVECOM – Soluções Rádio, S.A.
Dono do Documento	Information Security Manager (ISM)
Equipa de Segurança	Wavecom Product Security Incident Response Team (PSIRT) — em constituição. Até à sua constituição formal, a função é assegurada pelo Information Security Manager em conjunto com o Departamento de I&D.
Versão	1.0
Data de Entrada em Vigor	8 de setembro de 2026
Ciclo de Revisão	Anual, ou antes disso na sequência de alteração significativa do produto ou do enquadramento CRA aplicável
Classificação	Público

2. Objetivo

A WAVECOM assume o compromisso com a segurança dos produtos com elementos digitais que coloca no mercado. Esta **Política de Divulgação Coordenada de Vulnerabilidades (CVD)** descreve como terceiros — incluindo investigadores de segurança, clientes e o público em geral — podem reportar potenciais vulnerabilidades de segurança nos nossos produtos e sistemas, e como esses relatos são tratados.

Esta política está alinhada com o Regulamento (UE) 2024/2847 (Cyber Resilience Act — CRA) e com a prEN 40000-1-3, que estabelece requisitos e recomendações para os fabricantes de produtos com elementos digitais quanto à divulgação de potenciais vulnerabilidades.

3. Funções e Responsabilidades

> *UE 2024/2847 (CRA) — Art. 13.º(17): os fabricantes têm de designar um ponto de contacto único. O contacto tem de ser facilmente identificável, permitir que o utilizador escolha o meio de comunicação preferido e não pode limitar-se a ferramentas automatizadas.*

3.1 Equipa Interna de Segurança

A equipa interna responsável pela gestão da divulgação de vulnerabilidades é a Wavecom Product Security Incident Response Team (PSIRT), a quem compete:

Rececionar e acusar a receção das vulnerabilidades reportadas.

Validar, avaliar e priorizar as vulnerabilidades com base no risco.

Coordenar as atividades de correção com as equipas internas envolvidas.

Gerir a comunicação ao longo de todo o processo de tratamento da vulnerabilidade.

Emitir avisos de segurança e notificações de vulnerabilidade, quando aplicável.

Campo	Wavecom
Equipa ou pessoa responsável pela receção dos relatos	Information Security Manager (ISM), enquanto ponto de contacto único CRA, com monitorização de ciberseguranca@wavecom.pt.
Existe um PSIRT formal?	As atividades de cibersegurança estão atualmente distribuídas pela equipa técnica da Wavecom. Está prevista a constituição de um PSIRT dedicado.
Quem coordena a correção?	Departamento de I&D, em conjunto com o Product Security Owner da linha de produto afetada.
Quem aprova a divulgação pública?	Conselho de Administração, sob proposta do ISM.

3.2 O Que Pedimos a Quem Reporta Vulnerabilidades

Espera-se que qualquer pessoa ou organização que submeta um relato de vulnerabilidade atue de boa-fé e cumpra o seguinte:

- Não explorar a vulnerabilidade para além do necessário para confirmar a sua existência.
- Não aceder, alterar ou exfiltrar dados para além do estritamente necessário para demonstrar o problema.
- Não divulgar publicamente a vulnerabilidade antes de termos tido oportunidade razoável de a investigar e corrigir.
- Fornecer informação suficiente para reproduzirmos, avaliarmos e validarmos o problema reportado.
- Não realizar ataques de negação de serviço, engenharia social ou phishing no âmbito dos testes.

4. Âmbito da Política

> *CRA / prEN 40000-1-3 [PRE-2-RC-02]: a política de divulgação de vulnerabilidades deve especificar as opções de comunicação segura, o âmbito, a publicação, o reconhecimento e o conteúdo dos relatos. UE 2024/2847 (CRA) — Anexo I, Parte I, ponto (2)(a): os produtos têm de ser colocados no mercado sem vulnerabilidades exploráveis conhecidas, o que exige um processo de receção de relatos.*

4.1 Produtos e Sistemas Abrangidos

Os seguintes sistemas, produtos e serviços estão abrangidos por esta política:

Produto / Sistema	Versão / URL / Detalhe do âmbito	Inclui cloud / aplicação?
Wavecom IoT Gateway	Gamas WR, WK e WT — todas as revisões de hardware e versões de firmware suportadas colocadas no mercado da UE, incluindo unidades colocadas antes de 11 de setembro de 2026 (CRA, art. 69.°(3)). Sistema operativo executado no hardware Wavecom IoT Gateway série WR — WaveOS — versões 2025 e seguintes.	Sim — gerido através do Wavecom IoT Manager

Produto / Sistema	Versão / URL / Detalhe do âmbito	Inclui cloud / aplicação?
Wavecom IoT Manager	Plataforma web centralizada, em SaaS e on-premises — todas as versões suportadas, incluindo: Serviço de gestão e aprovisionamento de gateways; Serviço de gestão e aprovisionamento de dispositivos; Serviço de monitorização de frota; Serviço de monitorização de água.	Não
Cloud Authentication System (CAS)	Serviço de autenticação de visitantes Wi-Fi e controlo de acessos, em SaaS e on-premises, integrado na plataforma Wavecom IoT Manager ou autónomo.	Não
WHERE IS®	Plataforma de localização RTLS e RFID, incluindo os componentes de software desenvolvidos pela Wavecom, em SaaS e on-premises; o hardware de terceiros é coberto pelos respetivos fabricantes.	Não

4.2 O Que Não É Abrangido (Fora de Âmbito)

Ficam fora do âmbito desta política os elementos seguintes. Os relatos que lhes digam respeito não serão investigados:

- Produtos, serviços ou infraestruturas de terceiros não detidos nem operados pela Wavecom.
- Engenharia social, phishing ou ataques à segurança física da Wavecom ou dos seus colaboradores.
- Ataques de negação de serviço (DoS) ou de negação de serviço distribuída (DDoS).
- Produtos ou versões de software em fim de vida e já sem suporte.
- Vulnerabilidades já conhecidas da Wavecom ou já reportadas por terceiros.

5. Como Reportar uma Vulnerabilidade

> *UE 2024/2847 (CRA) — Art. 13.º(17): o ponto de contacto único tem de ser facilmente identificável, permitir que o utilizador escolha o meio de comunicação preferido e não pode limitar-se a ferramentas automatizadas. prEN 40000-1-3 [PRE-2-RQ-02]: tem de existir um ou mais mecanismos de contacto. [RCP-1-RQ-01]: os mecanismos de contacto têm de ser acessíveis ao público.*

5.1 Canais de Contacto

Canal	Obrigatório?	Detalhe
Endereço de e-mail de segurança	Obrigatório — caixa de correio monitorizada	ciberseguranca@wavecom.pt — caixa monitorizada, operada pelo Information Security Manager (ISM) enquanto ponto de contacto único CRA ao abrigo do art. 13.º(17). Aviso de receção em 3 a 5 dias úteis.
Telefone / apoio ao cliente	Opcional — útil quando já existe uma linha de apoio	O Apoio Técnico da Wavecom pode receber relatos através dos canais habituais de apoio ao cliente. As equipas de apoio e de engenharia de campo estão instruídas para encaminhar de imediato qualquer indício de vulnerabilidade de segurança ou de exploração ativa para ciberseguranca@wavecom.pt, e por telefone sempre que haja suspeita de exploração, sem avaliação técnica prévia.
Chave PGP (para e-mail cifrado)	Recomendada quando o e-mail é o canal principal — permite o envio seguro de informação sensível	Ainda não publicada. Quem necessite de transmitir informação sensível deve solicitar as condições de cifra em ciberseguranca@wavecom.pt.

5.2 O Que Deve Constar do Relato

> *CRA / prEN 40000-1-3 [PRE-2-RC-02]: a política de divulgação de vulnerabilidades deve especificar o conteúdo esperado dos relatos.*

Pedimos que, sempre que possível, o relato inclua no mínimo a informação seguinte, o que nos permite triar e investigar com rapidez:

- Nome, modelo, versão e/ou URL do produto afetado.

- Descrição clara da vulnerabilidade e do seu potencial impacto na segurança.
- Instruções passo a passo para reproduzir a vulnerabilidade, incluindo ferramentas e configurações utilizadas.
- Evidências de suporte — capturas de ecrã, capturas de rede, ficheiros de registo ou código de prova de conceito.
- Sugestão de gravidade ou pontuação CVSS, se disponível (opcional).
- Contactos para seguimento — os relatos anónimos também são aceites.

6. Tratamento de Vulnerabilidades

> *CRA / prEN 40000-1-3 [PRE-2-RQ-03]: as expectativas de comunicação com quem reporta têm de estar descritas. UE 2024/2847 (CRA) — Anexo I, Parte II, ponto (2): as vulnerabilidades têm de ser tratadas e corrigidas sem demora indevida, incluindo através da disponibilização de atualizações de segurança.*

6.1 Aviso de Receção

> *CRA / prEN 40000-1-3 [RCP-1-RQ-02]: a cada relato tem de ser atribuído um número de seguimento. [RCP-1-RQ-03]: o aviso de receção tem de ser enviado dentro do prazo indicado nesta política.*

Após a receção de um potencial relato de vulnerabilidade, a Wavecom acusa a receção no prazo indicado abaixo. O aviso de receção inclui um número de seguimento único.

A WAVECOM acusa a receção de todos os relatos de vulnerabilidade no prazo de 3 a 5 dias úteis. O aviso de receção inclui um número de seguimento único, que deve ser indicado em toda a correspondência subsequente.

6.2 Triagem e Verificação

> *CRA / prEN 40000-1-3 [VRF-1-RQ-01]: se o relato inicial não contiver informação suficiente para reproduzir a vulnerabilidade, quem reporta tem de ser contactado para prestar informação adicional.*

Após o aviso de receção, a equipa de segurança avalia o relato no prazo definido. Nessa avaliação, a Wavecom procede a:

- Validação e reprodução das vulnerabilidades reportadas.
- Avaliação da gravidade através de um sistema de pontuação estabelecido (CVSS v3.1).
- Identificação dos produtos e versões afetados.
- Atribuição de prioridade e do responsável pela correção.

Se o relato submetido não contiver informação suficiente para reproduzir a vulnerabilidade, a equipa de segurança contacta quem reportou para obter os elementos adicionais necessários.

A WAVECOM conclui a triagem inicial e presta informação sobre o estado do processo no prazo de 7 dias úteis a contar do aviso de receção. Quando o relato diga respeito a uma vulnerabilidade ativamente explorada, a triagem inicia-se de imediato e o processo de comunicação do artigo 14.º do CRA é ativado em paralelo, independentemente da comunicação com quem reportou.

6.3 Prazos de Correção

> *prEN 40000-1-3 [RMD-2-RQ-01]: a correção tem de ser desenvolvida. [RMD-3-RQ-01]: a correção tem de ser testada.*

A WAVECOM procura corrigir as vulnerabilidades validadas dentro dos seguintes prazos-alvo, em função da gravidade:

Gravidade	Prazo-alvo
Crítica / Elevada (CVSS ≥ 7,0)	30 dias de calendário
Média (CVSS 4,0 – 6,9)	60 dias de calendário
Baixa (CVSS < 4,0)	90 dias de calendário
Casos especiais (quando aplicável)	Equipamento no terreno que só pode ser atualizado em janela de manutenção programada e vulnerabilidades em componentes de terceiros a aguardar correção do fornecedor. Os prazos alargados são acordados previamente com quem reportou, justificados por escrito e registados.

Escala de Gravidade e Tempos de Resposta

BAIXA	MÉDIA	ELEVADA	CRÍTICA
CVSS 0,1–3,9 Prazo-alvo: 90 dias	CVSS 4,0–6,9 Prazo-alvo: 60 dias	CVSS 7,0–8,9 Prazo-alvo: 30 dias	CVSS 9,0–10,0 Prazo-alvo: 30 dias*

** As vulnerabilidades críticas sob exploração ativa são priorizadas para a correção mais rápida possível, mesmo antes do prazo-alvo de 30 dias.*

Sempre que a correção não possa ser disponibilizada dentro do prazo-alvo, a Wavecom informa previamente quem reportou, com uma data revista e, quando existam, orientações de mitigação provisória.

> *CRA / prEN 40000-1-3 [RMD-3-RQ-01]: a correção tem de ser testada antes da disponibilização, para confirmar que resolve a vulnerabilidade e não introduz novos problemas.*

Antes da disponibilização de qualquer correção, verificamos que esta resolve a vulnerabilidade reportada e não introduz novas fragilidades de segurança. Nas vulnerabilidades de gravidade crítica e elevada, os testes incluem verificação funcional e, quando adequado, testes de regressão.

6.4 Divulgação Pública Coordenada

Praticamos a divulgação coordenada: trabalhamos com quem reportou a vulnerabilidade para acordar a data de partilha pública da informação, assim que exista correção disponível.

> *CRA — Anexo I, Parte II, ponto (4): a informação sobre vulnerabilidades corrigidas tem de ser divulgada publicamente, incluindo descrição, versões afetadas, gravidade e orientações de correção. prEN 40000-1-3 [PRE-2-RC-02]: a política deve incluir o procedimento de publicação. [PRE-2-RC-03]: a divulgação tem de ser coordenada para evitar publicação prematura.*

A WAVECOM procura concluir a divulgação coordenada no prazo de 90 dias de calendário a contar da data do aviso de receção. Não sendo possível, contactamos quem reportou antes do termo do prazo para acordar uma nova data.

Importante — direito de divulgação: sempre que seja necessário para proteger os utilizadores ou para cumprir obrigações legais aplicáveis, a **WAVECOM** reserva-

se o direito de divulgar publicamente informação sobre a vulnerabilidade sem acordo prévio ou participação de quem reportou.

Sempre que ambas as partes acordem um período de embargo — período durante o qual nenhuma delas publica informação sobre a vulnerabilidade — o período acordado e a respetiva data de fim (data de divulgação) são documentados por escrito. Qualquer das partes pode pedir a prorrogação do embargo mediante justificação razoável.

Após a disponibilização da correção, a Wavecom:

- Informa quem reportou de que a vulnerabilidade foi resolvida.
- Publica um aviso de segurança, nota de versão ou notificação de produto.
- Credita quem reportou no aviso público, com o seu consentimento.

7. Plataforma Única de Comunicação (SRP)

> *Informação adicional: Regulamento (UE) 2024/2847, EUR-Lex, considerando (65).*

Definições

Vulnerabilidade ativamente explorada: incidente de segurança em que uma vulnerabilidade ativa no produto é explorada por um agente malicioso.

Incidente grave: incidente de segurança em que as funcionalidades de segurança do produto são significativamente afetadas e que não pode ser classificado como «vulnerabilidade ativamente explorada».

7.1 Mecanismos de recolha de informação

Canal	Definição	Detalhe
Consultas a clientes	Os clientes são periodicamente questionados sobre incidentes de segurança que envolvam os produtos.	Responsável: Departamento Comercial e Apoio Técnico. A segurança é incluída nas revisões periódicas de serviço ao cliente e nas intervenções no terreno. Os registos são mantidos no repositório de incidentes; qualquer indício de exploração é escalado de imediato ao ISM.
Threat Intelligence	Monitorização de fontes comerciais e abertas sobre exploração de vulnerabilidades	Avisos do CNCS e do CERT.PT, publicações da ENISA, feeds de CVE correlacionados com o inventário de componentes (SBOM) do WaveOS e das plataformas (IoT Manager, CAS e WHERE IS) e boletins de fornecedores e parceiros ODM/OEM (RAK, Supermicro, Kontron, Quectel, SimCom e fornecedores de cloud).
Submissão de vulnerabilidades	Avaliação das vulnerabilidades recebidas pelos canais de relato para determinar se estão a ser ativamente exploradas.	Os relatos recebidos em ciberseguranca@wavecom.pt ao abrigo desta política são triados pelo ISM, que determina se existe evidência fiável de exploração ativa.
Gestão interna de vulnerabilidades	Avaliação das vulnerabilidades identificadas internamente para determinar se estão a ser ativamente exploradas	Os resultados do ciclo de desenvolvimento seguro (SGSI_PLT10), dos testes internos e de terceiros e da monitorização e revisão de registos das plataformas SaaS (IoT Manager, CAS, WHERE IS®) são avaliados quanto a evidência de exploração ativa.
Outros		Escalamento interno: qualquer colaborador, prestador ou engenheiro de campo que receba um indício de exploração ativa comunica-o de imediato ao ISM, por escrito, sem avaliação técnica prévia e sem filtragem hierárquica.

7.2 Comunicações à ENISA

As comunicações seguintes são submetidas na plataforma única de comunicação da ENISA:

- https://portal.cra-srp.enisa.europa.eu/

Tipo de comunicação	**Prazo (a contar da deteção)**	**Conteúdo da comunicação**
Alerta precoce	24 h	Tipo de notificação (vulnerabilidade / incidente) Nível de notificação (24 h, 72 h, final) Nome do fabricante ou administrador Produto Título
Notificação de vulnerabilidade / incidente	72 h	Conteúdo do alerta precoce Natureza da vulnerabilidade Natureza da exploração Medidas corretivas ou de mitigação adotadas Medidas corretivas ou de mitigação que os utilizadores podem adotar Sensibilidade da informação (quando aplicável)
Relatório final (vulnerabilidades)	14 dias	Conteúdo da notificação de vulnerabilidade / incidente Data de disponibilização da medida corretiva ou de mitigação Descrição completa da vulnerabilidade Gravidade da vulnerabilidade Impacto da vulnerabilidade Agente malicioso que explorou a vulnerabilidade Detalhe da atualização de segurança / medidas corretivas disponíveis
Relatório final (incidentes graves)	1 mês	Conteúdo da notificação de vulnerabilidade / incidente Descrição detalhada do incidente Gravidade do incidente Impacto do incidente Tipo de ameaça ou causa-raiz que originou o incidente Medidas de mitigação aplicadas e em curso

8. Confidencialidade e Relatos Anónimos

> *prEN 40000-1-3 [PRE-5-RC-03]: quem reporta tem de poder submeter relatos de forma anónima.*

Todos os relatos de vulnerabilidade são tratados com confidencialidade. A informação pessoal fornecida por quem reporta não é partilhada com terceiros sem consentimento expresso, salvo quando exigido por lei aplicável.

Quem pretenda manter o anonimato pode submeter relatos por qualquer dos canais indicados, sem fornecer dados pessoais. Note-se que o anonimato pode limitar a nossa capacidade de dar informação sobre o estado do processo ou de conceder reconhecimento formal.

Os relatos anónimos são aceites e triados nos mesmos termos dos relatos identificados. Não sendo fornecidos contactos, não é possível pedir esclarecimentos, acordar uma data de divulgação coordenada ou prestar informação sobre o estado do processo.

9. Contactos

Campo	Detalhe
Contacto de segurança	ciberseguranca@wavecom.pt
Morada	WAVECOM – Soluções Rádio, S.A. Rua das Cardadeiras, 107 3800-125 Aveiro, Portugal
Chave pública PGP	Disponibilizada a pedido.
Horário de resposta	09:00–18:00 (Europa/Lisboa), de segunda a sexta-feira, exceto feriados nacionais. Os relatos que indiquem exploração ativa são escalados fora deste horário através do contacto de escalamento permanente.
Contacto de escalamento	Information Security Manager (ISM), enquanto ponto de contacto único CRA. Os contactos de escalamento estão documentados no SGSI_PLT19 (Lista de Contactos de Autoridades).

10. Gestão da Política

10.1 Revisão e Atualização

Esta política é revista pelo menos anualmente, ou antes disso na sequência de alteração significativa da gama de produtos, da equipa de segurança ou do enquadramento regulamentar. As versões atualizadas são publicadas no sítio da Wavecom e comunicadas internamente.

Campo	Wavecom
Onde será publicada esta política?	https://www.wavecom.pt/security (a confirmar), com um ficheiro security.txt em https://www.wavecom.pt/.well-known/security.txt e referência na documentação do produto.
Quem é responsável pela revisão?	Information Security Manager (ISM)
Próxima revisão	Setembro de 2027, ou antes disso na sequência de alteração significativa do produto ou do enquadramento CRA aplicável

10.2 Exceções

Qualquer exceção a esta política tem de ser aprovada pelo dono do documento e registada no registo de exceções. Todas as exceções são temporárias e revistas anualmente.

11. Histórico do Documento

Versão	Data	Autor	Descrição da alteração
1.0	8 de setembro de 2026	Information Security Manager (ISM)	Versão inicial, adaptada do modelo de política CVD da Eurofins v1.0