Política de Gerenciamento de Vulnerabilidades da Axis

Visão geral

Na condição de autoridade de numeração CVE (CNA), a Axis adota as práticas recomendadas da indústria, quanto ao gerenciamento e resposta a vulnerabilidades de segurança descobertas em nossos produtos. No entanto, não há como garantir que os produtos e serviços fornecidos pela Axis estejam totalmente livres de vulnerabilidades. E isso não é exclusividade da Axis, mas sim uma condição geral para todos os softwares e serviços. O que a Axis pode garantir é que envidaremos todos os esforços *em todas as etapas do desenvolvimento* para identificar e mitigar possíveis vulnerabilidades, minimizando assim o risco associado à implantação dos produtos e serviços da Axis nos ambientes dos clientes.

A Axis reconhece que certos protocolos e serviços de sistema em rede padrão podem apresentar vulnerabilidades inerentes que poderiam ser exploradas. Embora a Axis não se responsabilize por esses protocolos e serviços, oferecemos recomendações sobre como reduzir os riscos relacionados aos seus produtos, softwares e serviços da Axis por meio do nosso *guia para aumento do nível de proteção do AXIS OS*, do *guia para aumento do nível de proteção do AXIS Camera Station* e do *guia para aumento do nível de proteção dos switches de rede da Axis*.

Escopo

A política de gerenciamento de vulnerabilidades descrita neste documento se aplica a todos *os produtos, softwares e serviços da marca Axis*. Estão excluídos desta política os produtos, softwares e serviços 2N, gerenciados pela *equipe de segurança da 2N*.

Compromisso

A Axis valoriza e incentiva os esforços dos pesquisadores na identificação e notificação de vulnerabilidades nos produtos, softwares e serviços da Axis. Ao seguir o processo de divulgação responsável, a Equipe de Segurança de Produtos da Axis, na medida do possível, respeitará os interesses do pesquisador por meio da colaboração mútua e da transparência ao longo de todo o processo de divulgação.

A Axis espera que os pesquisadores não divulguem vulnerabilidades antes do término de um período de 90 dias ou de uma data mutuamente acordada e que realizem pesquisas sobre vulnerabilidades dentro dos limites legais, de forma a não causar danos, não expor a privacidade nem comprometer a segurança da Axis, seus parceiros e clientes.

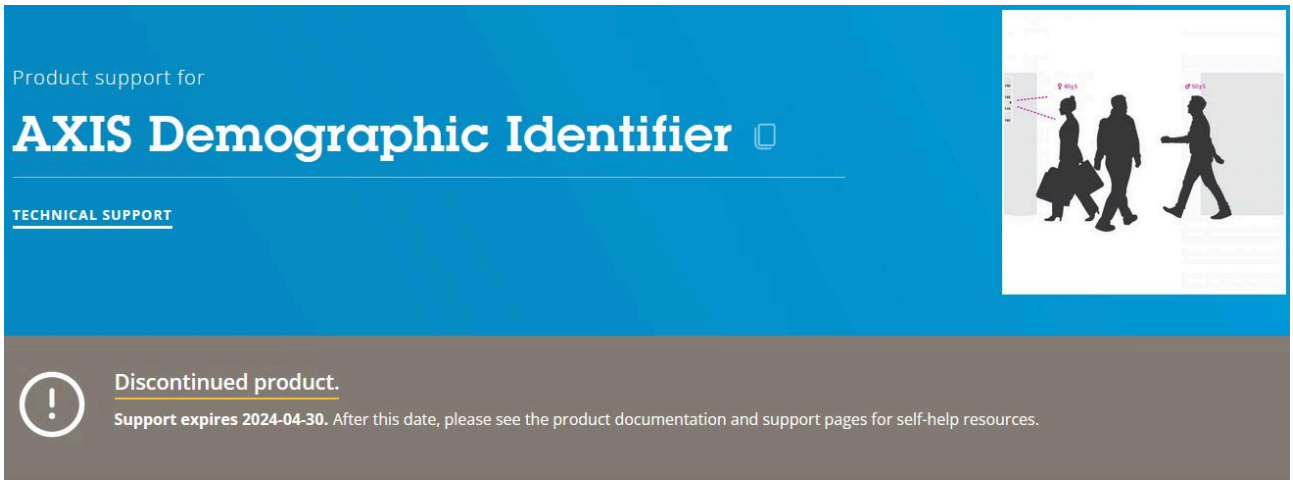
Gerenciamento de vulnerabilidades

A Axis utiliza a mesma classificação para *componentes de código aberto de terceiros* e para vulnerabilidades específicas da Axis. As vulnerabilidades são pontuadas por meio do conhecido *Common Vulnerability Scoring System* (CVSS). No que diz respeito às vulnerabilidades de código aberto, a Axis poderá avaliar a vulnerabilidade de acordo com sua relevância em relação às recomendações da empresa quanto à implantação de seus produtos, software e serviços. Normalmente, um aviso de segurança é emitido apenas para vulnerabilidades específicas da Axis. A seção a seguir descreve a priorização a ser seguida quando uma vulnerabilidade for avaliada e estiver apta a ser corrigida:

CVSS v4.0: alto/crítico (7,0 – 10,0)
A Axis tem como objetivo resolver a vulnerabilidade no prazo máximo de 4 semanas após a divulgação externa. No caso de componentes de código aberto, o prazo de entrega costuma ser mais longo, pois a Axis depende de terceiros para obter informações, correções e/ou verificação. A resolução de uma vulnerabilidade envolve a aplicação de uma correção no software ou a mitigação da vulnerabilidade por meio da desativação do componente ou da funcionalidade afetada.

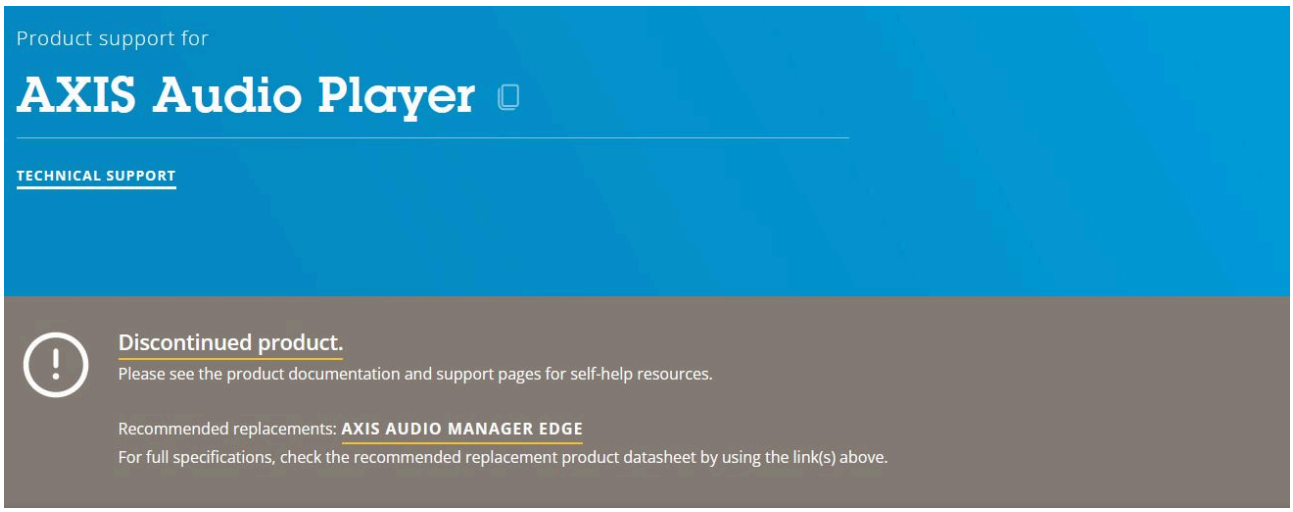
CVSS v4.0: baixo/médio (0,1 – 6,9)
As vulnerabilidades de nível baixo/médio geralmente acarretam consequências menos significativas para a segurança do produto, pois exigem acesso privilegiado ao dispositivo ou têm impacto limitado sobre a confidencialidade, a integridade ou a disponibilidade. Portanto, a Axis poderá corrigir a vulnerabilidade, eventualmente, como parte de uma próxima versão programada, caso seja considerado necessário. No caso de componentes de código aberto, o prazo de entrega costuma ser mais longo, pois a Axis depende de terceiros para obter informações, correções e/ou verificação. A resolução de uma vulnerabilidade envolve a aplicação de uma correção no software ou a mitigação da vulnerabilidade por meio da desativação do componente ou da funcionalidade afetada.

Software/serviços compatíveis
A fase de suporte de um software/serviço da Axis é definida por meio de um processo comum do ciclo de vida do software. O suporte ao software e aos serviços da Axis geralmente é mantido por três anos após o comunicado sobre a descontinuação.



Exemplo de um produto de software descontinuado que receberá suporte até 30 de abril de 2024.

Enquanto nessa fase, os softwares/serviços da Axis são considerados sob suporte até que atinjam a fase de softwares/serviços descontinuados.



Exemplo de um produto de software descontinuado, conforme pode ser encontrado no site axis.com.

Produtos com suporte
O suporte a um produto da Axis é definido por meio do *processo comum de ciclo de vida de produto de hardware*. Os produtos da Axis são considerados sob suporte até que atinjam a fase de Produto descontinuado. Fase: apenas suporte on-line

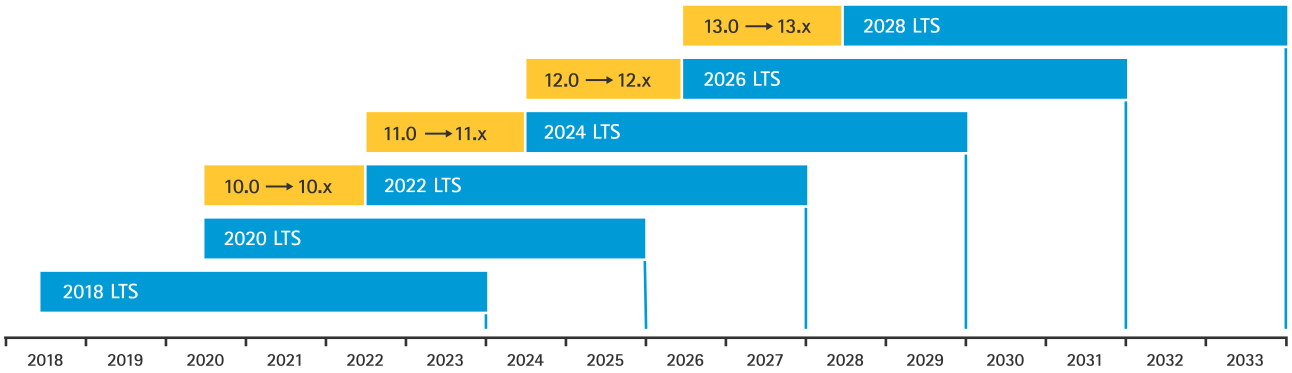
É possível obter informações sobre o estado atual dos produtos da Axis na página correspondente do produto Axis, no site *www.axis.com*. Mais informações sobre a política geral de suporte após a descontinuação de um produto podem ser encontradas *aqui*.



Exemplo de um produto de hardware descontinuado, conforme pode ser encontrado no site axis.com.

O AXIS OS é o sistema operacional que alimenta a maioria dos produtos de rede da Axis. Para muitos produtos, a Axis oferece suporte estendido ao software por meio das versões de suporte de longo prazo (LTS) do AXIS OS. A utilização da linha LTS pode prolongar o suporte ao ciclo de vida geral de um produto da Axis. Saiba mais sobre o AXIS OS *aqui*.

Visão geral do suporte ao OS AXIS



A linha de desenvolvimento ativa lança uma nova versão a cada dois meses, sendo que apenas a versão mais recente tem suporte. As versões LTS são criadas a cada dois anos e recebem suporte e manutenção por cerca de 5 anos.

Versões do AXIS OS LTS atualmente compatíveis e versões em desenvolvimento (em outubro de 2023).

Notificação de vulnerabilidades

A Axis trabalha continuamente para identificar e minimizar os riscos associados às vulnerabilidades em nossos produtos. No entanto, caso identifique uma vulnerabilidade de segurança associada a um produto, software ou serviço da Axis, recomendamos que você comunique o problema imediatamente. A comunicação oportuna de vulnerabilidades de segurança é fundamental para reduzir a probabilidade de que elas sejam exploradas na prática. As vulnerabilidades de segurança relacionadas a componentes de software de código aberto devem ser comunicadas diretamente à entidade responsável.

Incentivamos usuários finais, parceiros, fornecedores, grupos do setor e pesquisadores independentes que tenham identificado uma possível vulnerabilidade a enviar suas descobertas por meio *deste formulário*. A notificação apresentada deve incluir:

- Informações técnicas sobre a possível vulnerabilidade.
- Passos para reprodução.
- *Pontuação CVSS v3.1 estimada e string vetorial resultante*.
- Uma sugestão de correção.
- A política de divulgação de vulnerabilidades do próprio pesquisador, se disponível.

É possível esperar os seguintes tempos de resposta da Axis:

- O prazo para a primeira resposta é de até 2 dias úteis após o recebimento do envio inicial.
- O tempo até a triagem (a partir do momento da primeira resposta) é de até 10 dias úteis.

A Axis colabora com a Bugcrowd para oferecer *programas de recompensa por falhas (Bug Bounty)* para produtos baseados no AXIS OS. Convidamos pesquisadores de segurança e hackers éticos a participar desses programas. Para participar do nosso programa privado de recompensa por falhas, envie uma solicitação por meio do *processo de notificação de vulnerabilidades*. Outros produtos, software e serviços da Axis não fazem parte, no momento, de nenhum programa de recompensa por falhas.

Como forma de agradecimento, pesquisadores de segurança e hackers éticos que contribuírem com descobertas valiosas poderão receber reconhecimento público em nossos alertas de segurança e no *Hall of Fame*.

Divulgação de vulnerabilidades

Assim que uma descoberta relatada for investigada e confirmada como uma vulnerabilidade legítima, a Axis atribui um ID CVE e inicia o processo de divulgação responsável. A Axis se empenha em colaborar com pesquisadores de segurança para fornecer mais detalhes, como a pontuação CVSS v3.1, o conteúdo do comunicado de segurança e/ou dos comunicados à imprensa (se aplicável), e chega a um acordo sobre a data de divulgação externa.

A Axis segue um ciclo estruturado de divulgação trimestral de CVE, que ocorre na segunda terça-feira de fevereiro, maio, agosto e novembro. Este cronograma serve como o prazo padrão para a divulgação pública de vulnerabilidades validadas, o que inclui o envio do ID CVE à MITRE e a publicação do comunicado de segurança ou do comunicado à imprensa referente aos produtos e serviços da Axis afetados. Divulgações extraordinárias podem ser feitas, caso consideradas necessárias. As divulgações só são feitas quando há CVEs a serem divulgados.



Vulnerabilidades fora do escopo

Algumas vulnerabilidades estão fora do escopo da política de gerenciamento de vulnerabilidades da Axis. Não envie relatórios sobre vulnerabilidades fora do escopo da lista abaixo para *product-security@axis.com*.

- **Vulnerabilidades relacionadas ao sequestro de DLLs e ao carregamento paralelo de DLLs** em aplicações de software da Axis sendo executadas no sistema operacional Microsoft Windows. Para obter mais informações, consulte o *artigo a seguir*.
- **Vulnerabilidades que exigem privilégios elevados e/ou engenharia social**, que são iniciadas/executadas com acesso de root/administrador e/ou exigem interações complexas do usuário.
- **Apropriações de domínios**, como obtenção do controle de um host que aponta para um serviço que não está em uso no momento.
- **Erros de configuração do usuário** que poderiam ser evitados seguindo os guias para aumento do nível de proteção da Axis:
  - *Guia para aumento do nível de proteção do AXIS OS*
  - *Guia para aumento do nível de proteção do Sistema do AXIS Camera Station*
  - *Guia para aumento do nível de proteção dos switches de rede da Axis*
- **Vulnerabilidades em conteúdo ou aplicativos criados por usuários ou parceiros terceirizados**, como, por exemplo, os ACAPs que podem ser enviados e executados em dispositivos Axis.
- **Vulnerabilidades do tipo falsificação de solicitação entre sites (CSRF) ou scripting entre sites (XSS)** que induzem o usuário a acessar um site malicioso ou clicar em um link disfarçado enquanto realiza o acesso à interface web dos dispositivos Axis. Para obter mais informações, consulte o *aviso de segurança a seguir*.
- **Qualquer ataque do tipo DoS**; exemplos disso são:
  - Esgotamento dos recursos de um dispositivo devido ao uso normal da API com entradas de parâmetros modificadas.
  - Esgotamento de recursos devido a chamadas de API em alta frequência.
  - Esgotamento de recursos por meio de ataques do tipo slowloris.
- **Vulnerabilidades de código aberto de terceiros**, registradas com um ID CVE, localizadas em componentes ou pacotes de software utilizados nos produtos, softwares ou serviços da Axis. Exemplos comuns desses componentes de software são o kernel do Linux, o OpenSSL, o Apache e outros.
- **Cabeçalhos de segurança HTTP(S) ausentes**, como o X-Frame-Options.
- **Relatórios de vulnerabilidades gerados** por scanners de segurança em rede de terceiros.
- **Produtos/software/serviços sem suporte** que atingiram o estado de "Produto descontinuado". Fase: somente suporte online".
- **Problemas relatados que não documentam claramente uma falha real e explorável com impacto na segurança.** Por exemplo, a incompatibilidade entre erros no aplicativo e códigos de resposta HTTP ao realizar teste de estresse de API.

Serviço de notificação de segurança

A Axis publica diretrizes, alertas de segurança e comunicados sobre a *Política de Gerenciamento de Vulnerabilidades da Axis*. Além disso, é possível obter informações inscrevendo-se no serviço de notificações de segurança da Axis, disponível na página *Serviço de notificações de segurança*.

São enviadas notificações sobre vulnerabilidades específicas da Axis, independentemente da pontuação CVSS v4.0. As vulnerabilidades analisadas pela Axis estão documentadas nos *Avisos de Segurança do AXIS OS*.

T10185928_pt

2026-01 (M16.2)

© 2022 – 2026 Axis Communications AB