

Troubleshooting de Verificação de Integridade do Código de Erro de Módulo com Falha na Integração XDR de Acesso Seguro

Contents

Problema

A integração do Cisco Secure Access com o XDR falha com um erro HTTP 431 "Request Header Fields Too Large" (Campos de cabeçalho de solicitação muito grandes) durante a fase de verificação de integridade. A integração tinha funcionado anteriormente com êxito, mas repentinamente começou a falhar com esse erro ao tentar estabelecer a conexão usando chaves de API geradas a partir do painel do Cisco Secure Access.

A mensagem de erro específica é exibida como:

<#root>

Health check of Module failed: - [v2 Reporting API] There was a client error in the Cisco Secure Access

Esse erro impede que os dados do Secure Access sejam incluídos no XDR, afetando a visibilidade de segurança e os recursos de monitoramento.

Ambiente

- Cisco Secure Access com licença Advantage
- assinatura Cisco XDR
- Locatário do Cisco Secure Access
- Integração de API usando as chaves geradas pelo painel do Cisco Secure Access

- Escopos de API necessários: Investigar > Somente Leitura, Relatórios > Somente Leitura, Implantações > Somente Leitura, Políticas > Leitura/Gravação

Resolução

O problema foi resolvido com a regeneração da chave e do segredo da API no Cisco Secure Access.

Siga estas etapas para resolver o erro 431:

Passo 1: Gerar novas chaves de API

Navegue até o painel do Cisco Secure Access e crie novas chaves de API com os escopos necessários:

- Investigar: Somente leitura
- Relatórios: Somente leitura
- Implantações: Somente leitura
- Políticas: Leitura/Gravação

Passo 2: Aplicar novas chaves à integração do XDR

Substitua as chaves de API existentes na configuração de integração do Acesso Seguro XDR pelas chaves recém-geradas.

Passo 3: Verificar integração

Teste a integração para confirmar a conexão bem-sucedida. As chamadas de API devem agora retornar respostas HTTP 200 em vez do erro 431.

Detecção e prevenção proativas

Para identificar e evitar erros 431 semelhantes no futuro:

1.- Ao depurar através de ferramentas como Postman ou console do navegador, verifique a coluna de tamanho para cabeçalhos de solicitação. Se os cabeçalhos de solicitação se aproximarem ou excederem 8 KB (8192 bytes), isso acionará um erro 431 nos gateways de API. Ferramentas externas como jwt.io podem ser usadas para verificar o tamanho do token OAuth.

2.- Analisar padrões de erro:

- Se o erro 431 ocorrer instantaneamente durante o handshake inicial de uma verificação de integridade, ele indica que as credenciais estáticas são o problema
- Se o erro 431 ocorrer somente após a execução da integração por vários minutos, ele aponta para acúmulo de cookies em repetições subsequentes

Melhores práticas

Desabilite a persistência de cookie ou sessão no navegador/cliente de integração para evitar o acúmulo de tamanho de cabeçalho.

Causa

O erro HTTP 431 foi causado pela chave de API específica e pelo par secreto, gerando um cabeçalho de autorização grande ou malformado de forma incomum, quando a Base64 foi codificada para o cabeçalho de Autorização HTTP padrão.

As cadeias de caracteres criptográficas na chave de API inicial continham uma sequência de caracteres que, quando codificados, se expandiam em um tamanho de cabeçalho que excedia os limites do gateway de API, resultando na rejeição "Request Header Fields Too Large".

Quando a chave de API foi gerada novamente, a nova cadeia criptográfica produziu um cabeçalho de autorização de tamanho adequado. O processo de revogação e geração de uma nova chave também limpou o contexto de solicitação em cache no lado do gerenciador de

integração, normalizando o tamanho do cabeçalho.

Conteúdo relacionado

- [Autenticação de API do Cisco Secure Access](#)
- [Integração de acesso seguro da Cisco no XDR](#)
- [Coletar registros HAR do console XDR](#)
- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.