

# RELATÓRIO TESTE DE SEGURANÇA

WSS{pilot\_report\_found}



### 1. SUMÁRIO EXECUTIVO

Este relatório descreve a análise que foi conduzida no ativo **PILOT**, que, como prova de conceito, pode ser executado localmente tanto para análise, quanto auditorias futuras. Durante os diversos testes realizados, foi identificado a existência do software de armazenamento de objetos compatível com padrão *Amazon S3* conhecido como *MinIO*. Este software funciona de forma semelhante ao serviço de armazenamento em nuvem da AWS, mas pode ser instalado e executado localmente ou em nuvem privada de forma *self hosted*. Ele permite o armazenamento de grandes volumes de dados (arquivos, imagens, vídeos, backups, logs, etc.) de forma escalável e distribuída, usando uma interface simples baseada em APIs REST.

A implementação do *MinIO* identificada pertencente a faixa de versão entre a *RELEASE*.2019-12-17T23-16-33Z e a *RELEASE*.2023-03-20T20-16-18Z. Nesta versão, o *MinIO* possui uma vulnerabilidade pública conhecida (*CVE*-2023-28432¹) com prova de conceito disponibilizada no github. Essa vulnerabilidade permite um agente de ameaças retornar todas as variáveis de ambiente sem a necessidade de autenticação, incluindo *MINIO\_SECRET\_KEY* e *MINIO\_ROOT\_PASSWORD*, resultando numa divulgação de informações sensíveis. Todos os usuários de implantações distribuídas são impactados. Recomenda-se que todos os usuários façam a atualização para a versão *RELEASE*.2023-03-20T20-16-18Z. Mais detalhes estão descritos na descoberta PILOT-01.

Ainda, em posse dessas credenciais *root*, um agente de ameaça poderia explorar a segunda vulnerabilidade, descrita na descoberta <u>PILOT-02</u>. Essa vulnerabilidade (CVE-2023-28434²), identificada na mesma versão do *MinIO*, permite um usuário autenticado substituir o binário em execução por um binário malicioso, resultando em uma execução remota de código (*RCE*) no *host*.

Isoladas, essas duas descobertas são classificadas como altas pelo cálculo de CVSS. A segunda vulnerabilidade, do RCE, só não é classificada como crítica porque necessita de uma credencial de baixo nível de acesso (Privilege Required: Low). Contudo, quando exploradas em sequência, essas falhas possibilitam a extração das credenciais administrativas via CVE-2023-28432 e o posterior abuso da funcionalidade de atualização para obter execução arbitrária de comandos no servidor via CVE-2023-28434, comprometendo completamente a confidencialidade, integridade e disponibilidade do servidor e dos dados presentes nele.

<sup>&</sup>lt;sup>1</sup> NIST - CVE-2023-28432

<sup>&</sup>lt;sup>2</sup> NIST - CVE-2023-28434



#### 2. RESUMO DAS DESCOBERTAS

O resumo das descobertas encontradas é apresentado na Tabela 1 por meio da métrica quantitativa relacionada com o nível de criticidade.

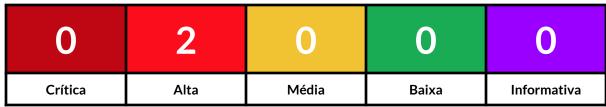


Tabela 1 - Resumo quantitativo de vulnerabilidades encontradas

Com base nas quantidades informadas acima, a Tabela 2 descreve cada uma das descobertas apontadas e possíveis formas abrangentes de mitigação.

ID	DESCRIÇÃO	CRITICIDADE
PILOT-01	Divulgação de Dados Sensíveis no MinIO	Alta
PILOT-02	Execução Remota de Código no MinIO	Alta

Tabela 2 - Resumo descritivo das descobertas



# 3. SUMÁRIO TÉCNICO DAS DESCOBERTAS

## 3.1. Divulgação de Dados Sensíveis no MinIO (PILOT-01)

Criticidade	7.5   Alta
CVSS 3.1	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Descrição	Uma falha na validação de requisições <i>POST</i> para um endpoint específico da <i>API</i> permite que um atacante obtenha variáveis de ambiente do servidor. Entre as informações vazadas estão as credenciais de acesso root, especificamente <i>MINIO_ROOT_USER</i> e <i>MINIO_ROOT_PASSWORD</i> . Esta descoberta não exige autenticação, o que eleva a criticidade de média para alta.
Local	http://localhost:9001
Referências	https://nvd.nist.gov/vuln/detail/cve-2023-28432 https://blog.min.io/security-advisory-stackedcves

## 3.2. Execução Remota de Código no MinIO (PILOT-02)

Criticidade	8.8   Alta	
CVSS 3.1	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	
Descrição	Foi descoberta a possibilidade de execução de código remoto ( <i>RCE</i> ) no servidor. Um agente de ameaça pode subverter a funcionalidade de atualização de configuração ( <i>admin-update</i> ), fazendo com que o servidor execute um binário arbitrário e potencialmente malicioso.  Em si, essa descoberta é classificada pela <i>NIST</i> como alta, pois leva em consideração a necessidade de uma credencial de acesso com baixos privilégios. Contudo, a descoberta <u>PILOT-01</u> eleva significativamente a criticidade dessa descoberta, pois torna possível obter credenciais de alto nível sem a necessidade de autenticação.	
Local	http://localhost:9000	
Referências	https://nvd.nist.gov/vuln/detail/cve-2023-28434 https://blog.min.io/security-advisory-stackedcves	



