WSS

A SEGURANÇA DIGITAL DO SEU MUNDO

RELATÓRIO

TESTE DE SEGURANÇA

PILOT

1. SUMÁRIO EXECUTIVO

Esta análise foi conduzida para avaliar a segurança na máquina local onde o **PILOT** está rodando. Durante os testes foi identificado que a existência de um **MinIO**, um software de armazenamento de objetos compatível com o padrão Amazon S3 - este funciona de forma semelhante ao serviço de armazenamento em nuvem da AWS, mas pode ser instalado e executado localmente ou em nuvem privada. 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.

Na 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**, o MinIO possui uma vulnerabilidade (**CVE-2023-28432**) que retorna todas as variáveis de ambiente, incluindo `MINIO_SECRET_KEY` e `MINIO_ROOT_PASSWORD`, resultando em **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. Dessa forma, a vulnerabilidade identificada trata de uma falha na validação de requisições POST para um endpoint de API que possibilita o vazamento de variáveis de ambiente do servidor.

Além da vulnerabilidade anteriormente citada, foi encontrada uma *flag* com valor *WSS{pilot_report}* e também outra vulnerabilidade decorrente da mesma versão do MinIO que permite que um usuário autenticado, aproveitando a funcionalidade de atualização administrativa (admin-update), faça com que o servidor substitua o binário em execução por um binário malicioso preparado pelo atacante, resultando em execução remota de código (RCE) no host. Assim, 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**.

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.

0	2	0	0	0
Crítica	**Alta**	**Média**	**Baixa**	**Informativa**

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 POST para um endpoint específico da API permite que um atacante obtenha variáveis de ambiente do servidor. Entre as informações vazadas estão as credenciais de acesso root, especificamente `MINIO_ROOT_USER` e `MINIO_ROOT_PASSWORD`. Esta vulnerabilidade não exige autenticação.
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	Após obter as credenciais de administrador, como citado na descoberta 3.1, um atacante autenticado pode abusar da funcionalidade de atualização de configuração (admin-update). Ao manipular o processo de atualização, é possível enganar o servidor para que ele execute um binário malicioso, resultando em execução remota de código no host.
Local	• http://localhost:9000
Referências	https://nvd.nist.gov/vuln/detail/cve-2023-28434 https://blog.min.io/security-advisory-stackedcves