TLP: CLEAR

BOLETIM DE SEGURANÇA

Backdoors e Cryptojacking: Exploração de vulnerabilidade crítica no Aviatrix Controller

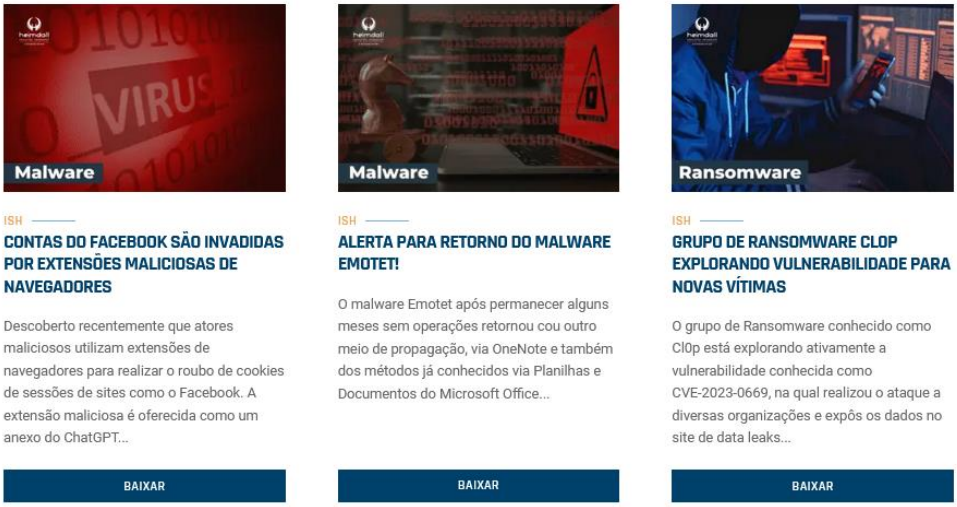
heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 INTRODUÇÃO EXECUTIVA

Este relatório de segurança, desenvolvido pela equipe de **Inteligência de Ameaças da ISH, Heimdall**, tem como objetivo proporcionar uma compreensão aprofundada e um dimensionamento preciso das ameaças cibernéticas identificadas. O documento está estruturado em três níveis de abordagem: ***Estratégico***, ***Tático*** e ***Operacional***, garantindo uma visão completa e integrada das ameaças e ações recomendadas.

2 ESTRATÉGICO

2.1 SEGMENTO DE MERCADO

Os segmentos de mercado potencialmente afetados por essa ameaça que será descrita neste relatório, incluem:

- *Provedores de serviços em nuvem*
- *Instituições financeiras*
- *Saúde e farmacêuticas*
- *Energia e Infraestrutura crítica*
- *Varejo*

IMPACTO FINANCEIRO POTENCIAL

- *Aumento dos custos com recursos em nuvem*
- *Perdas financeiras por exfiltração de dados*
- *Custos com resposta a incidentes e forense digital*

3 TÁTICO

3.1 INFORMAÇÕES SOBRE A FALHA E AMEAÇA

A vulnerabilidade crítica CVE-2024-50603, que afeta o **Aviatrix Controller**, representa uma ameaça significativa para ambientes cloud, especialmente aqueles implantados em **AWS**. A falha foi descoberta em outubro de 2024 e publicamente divulgada em janeiro de 2025. Desde então, tem sido explorada ativamente por grupos maliciosos que buscam comprometer infraestruturas corporativas em nuvem por meio de **execução remota de código não autenticada**. A exploração dessa vulnerabilidade ocorre em dois vetores principais de ataque: a **implantação de backdoors** para garantir persistência no ambiente e a **utilização de recursos computacionais** para mineração de criptomoedas. O malware utilizado pelos invasores inclui o minerador **XMRig** e o framework de comando e controle **Sliver**, garantindo controle contínuo sobre os sistemas comprometidos.

A vulnerabilidade está presente em versões anteriores à **7.1.4191** e **7.2.4996** do Aviatrix Controller. Durante a exploração, os atacantes se aproveitam de permissões padrão **IAM** em ambientes AWS para realizar **escalada de privilégios**, possibilitando acesso a planos de controle administrativos. Essa capacidade de movimentação lateral e o acesso privilegiado permitem que os atacantes comprometam **dados críticos** e **informações confidenciais** dos ambientes em nuvem das vítimas. Conforme a Wiz, os invasores estão utilizando técnicas de **enumeração de permissões cloud**, preparando-se para **exfiltração de dados** e potencial venda de acessos comprometedores a outros grupos criminosos. A exploração tem sido amplamente utilizada para cryptojacking, mas a possibilidade de ataques mais sofisticados não pode ser descartada. Com a publicação de uma prova de conceito (PoC), a vulnerabilidade pode ser rapidamente adotada por outros atores maliciosos, aumentando os riscos para as organizações.

3.2 OUTROS DETALHES DA VULNERABILIDADE

A falha decorre da neutralização inadequada de entradas fornecidas pelo usuário em endpoints API específicos, como *list_flightpath_destination_instances* e *flightpath_connection_test*, que tratam parâmetros sem a devida higienização. Essa vulnerabilidade permite a execução arbitrária de comandos no sistema operacional, oferecendo acesso remoto e controle total ao atacante.

O potencial de exploração aumenta significativamente em ambientes AWS, onde o Aviatrix Controller recebe permissões administrativas padrão de IAM por meio das funções atribuídas. Essa configuração facilita a escalada de privilégios e a movimentação lateral dentro do ambiente cloud, representando um risco elevado de comprometimento de dados e exfiltração de informações sensíveis.

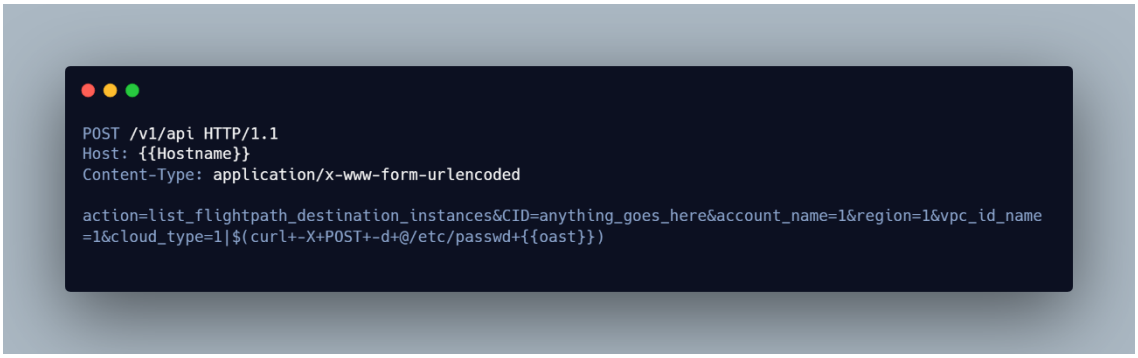


Figura 1 – Exploração da CVE-2024-50603 via endpoint /v1/api.

3.3 CAPACIDADE DA AMEAÇA

A exploração da vulnerabilidade no Aviatrix Controller evidencia uma capacidade avançada de manipulação de infraestruturas cloud por parte de atores mal-intencionados. Esse tipo de ameaça não apenas compromete servidores e dispositivos, mas também explora brechas em permissões e políticas de acesso, potencializando o impacto das ações maliciosas. A capacidade de realizar ataques automatizados e de alta escala demonstra que o objetivo não é apenas comprometer um sistema específico, mas explorar a superfície de ataque inteira de uma organização, tornando-se uma ameaça abrangente. Além disso, a sofisticação dos ataques inclui **injeção de comandos**, que pode ser utilizada para manipular dados, interromper serviços e criar vetores para futuras explorações.

4 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da exploração da vulnerabilidade, como por exemplo:

Aplicar patches de segurança imediatamente

- Atualize o Aviatrix Controller para as versões corrigidas 7.1.4191 ou 7.2.4996, conforme indicado pela documentação oficial.

Restringir o acesso público ao controlador

- Configure regras de firewall para impedir que a API do Aviatrix Controller esteja exposta à internet, protegendo a porta 443.

Revisar e ajustar permissões IAM

- Garanta que as permissões atribuídas ao Aviatrix Controller em ambientes AWS sejam mínimas e específicas, evitando que ele tenha acesso administrativo desnecessário.

Monitorar logs de API para atividades suspeitas

- Configure sistemas de detecção para identificar tentativas de exploração, como solicitações não autenticadas para endpoints vulneráveis.

Realizar investigação forense em ambientes comprometidos

- Caso haja suspeita de exploração, conduza uma análise detalhada dos sistemas para identificar backdoors e evidências de movimentação lateral.

Implementar autenticação multifator (MFA)

- Garanta que o acesso administrativo ao Aviatrix Controller esteja protegido por MFA, reduzindo o risco de comprometimento.

Estabelecer políticas de acesso seguras

- Implemente políticas rigorosas de controle de acesso que limitem a exposição de APIs críticas e garantam que apenas usuários e dispositivos autorizados possam interagir com o Aviatrix Controller.

5 OPERACIONAL

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Comprometimento (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

5.1 INDICADORES DE COMPROMETIMENTO (IOC)

Indicadores do artefato	
md5:	d19a46dc3ab5e207b75273ef6cdbd595
sha1:	1ce0c293f2042b677cd55a393913ec052eded4b9
sha256:	9a891b8edf7046a2c1aea92910a07955b432a3049792578c8fc41c6d2479bf03
File name:	15147153

Indicadores do artefato	
md5:	70ce2b359ecd9fe1538c34f503ac369d
sha1:	68d88d1918676c87dcd39c7581c3910a9eb94882
sha256:	cea67033ab3af68f964d27f43e5a30810d94d9902de1bb2004e477471520c038
File name:	xmrig

Indicadores do artefato	
md5:	923be511530054e563c0ace66cd3861e
sha1:	c4f63a3a6cb6b8aae133bd4c5ac6f2fc9020c349
sha256:	e638db05332e0beb528ca1f742094c54853fe347fe76e5a678f891e318104c8d
File name:	apache2

Indicadores do artefato	
md5:	6cde7499e4a86550b1f5d24738d988c3
sha1:	c63f646edfddb4232afa5618e3fac4eee1b4b115
sha256:	e0a4c5dbb6c10b7be03336b4d17ee56401f2a29263683093b8cd19c813acad37
File name:	udiskssd

Indicadores do artefato	
md5:	baba11542f150a65b4d6e1f683f72fa3
sha1:	e10e750115bf2ae29a8ce8f9fa14e09e66534a15
sha256:	8975c309893beecbb369c0cb9ffe7368a2a9607a02a0aea8f659fc58fb006e6e
File name:	config

Tabela 1 – Indicadores de Comprometimento

5.2 INDICADORES DE URL, IPS E DOMÍNIOS

Indicadores de IPs e Domínios	
IP	91.193[.]19[.]109

Tabela 2 – Indicadores de Comprometimento de Rede.

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **AVIATRIX**
- **NVD**
- **TheHackerNews**
- **Wiz Research**

7 AUTORES

- **Wesley Murat**

heimdall
security research
A DIVISION OF ISH