



APACHE

BOLETIM DE SEGURANÇA

**Atualizações de segurança da Apache para MINA,
HugeGraph e Traffic Control**

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



ISH

CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR



ISH

ALERTA PARA RETORNO DO MALWARE EMOTET!

O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR



ISH

GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS

O grupo de Ransomware conhecido como CLOP está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

SUMÁRIO

1	Informações sobre as vulnerabilidades.....	5
2	Recomendações.....	6
3	Referências	7
4	Autores.....	7

LISTA DE TABELAS

Tabela 1 – Versões afetadas e corrigidas do Apache MINA.	5
Tabela 2 – Versões afetadas e corrigidas do Apache HugeGraph-Server.....	5
Tabela 3 – Versões afetadas e corrigidas do Apache Traffic Control	5

1 INFORMAÇÕES SOBRE AS VULNERABILIDADES

A Apache Software Foundation [lançou](#) atualizações de segurança para corrigir três vulnerabilidades críticas nos produtos **MINA**, **HugeGraph-Server** e **Traffic Control**. As novas versões do software, lançadas entre 23 e 25 de dezembro, abordam essas falhas, no entanto, devido ao período de férias, a aplicação dos patches pode ser mais lenta, aumentando o risco de exploração.

A [CVE-2024-52046](#) trata-se de uma vulnerabilidade que possibilita o atacantes aproveitem o processo de desserialização ao enviar dados maliciosos especialmente formatados, o que pode resultar em ataques de execução remota de código (RCE). Este problema impacta as versões principais do MINA 2.0.X, 2.1.X e 2.2.X, e será resolvido nas versões 2.0.27, 2.1.10 e 2.2.4. Vale destacar que um aplicativo que utiliza a biblioteca principal do MINA só será afetado se o método `loBuffer#getObject()` for chamado. Esse método pode ser acionado ao adicionar uma instância de `ProtocolCodecFilter` usando a classe `ObjectSerializationCodecFactory` na cadeia de filtros.

Versões afetadas	Versões corrigidas
MINA 2.0.X, 2.1.X e 2.2.X	MINA 2.0.27, 2.1.10 e 2.2.4

Tabela 1 – Versões afetadas e corrigidas do Apache MINA.

A [CVE-2024-43441](#) refere-se a uma vulnerabilidade de Bypass no Apache HugeGraph-Server que permite o a autenticação devido a dados considerados imutáveis. Esta falha afeta as versões do Apache HugeGraph-Server desde a 1.0.0 até a 1.4.9.

Versões afetadas	Versões corrigidas
Apache HugeGraph-Server 1.0 e 1.3	Apache HugeGraph-Server 1.5.0

Tabela 2 – Versões afetadas e corrigidas do Apache HugeGraph-Server.

A [CVE-2024-45387](#) refere-se a uma falha de segurança de injeção de SQL foi identificada no Traffic Ops do Apache Traffic Control nas versões 8.0.0 a 8.0.1. Essa vulnerabilidade permite que usuários com funções privilegiadas, como "admin", "federation", "operations", "portal" ou "steering", executem comandos SQL arbitrários no banco de dados ao enviar uma solicitação PUT especialmente formatada.

Versões afetadas	Versões corrigidas
Apache Traffic Control 7.0.0, 8.0.0 até 8.0.1	Apache Traffic Control 8.0.2

Tabela 3 – Versões afetadas e corrigidas do Apache Traffic Control.

2 RECOMENDAÇÕES

Como informado acima, recomendamos que os administradores de sistema atualizem para a versão mais recente do produto o quanto antes. Isso é especialmente importante nesta época do ano, pois hackers tendem a atacar quando há menos funcionários disponíveis e os tempos de resposta são mais lentos.

3 REFERÊNCIAS

- Heimdall *by* ISH Tecnologia
- [Apache](#)
- [Bleepingcomputer](#)
- [NVD](#)

4 AUTORES

- Leonardo Oliveira Silva



heimdall
security research

A DIVISION OF ISH