TLP: CLEAR

BOLETIM DE SEGURANÇA

Falha grave no Splunk expõe sistema à Execução Remota de Código (RCE)

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

1 SUMÁRIO EXECUTIVO

A plataforma **Splunk**, amplamente utilizada para análise e monitoramento de dados, enfrenta uma vulnerabilidade de **Execução Remota de Código (RCE)**. Catalogada como **CVE-2024-53247**, a falha impacta diversas versões do **Splunk Enterprise** e do aplicativo **Splunk Secure Gateway** na **Splunk Cloud Platform**. Classificada como grave, essa vulnerabilidade representa um risco significativo para organizações que utilizam esses serviços.

2 INFORMAÇÃO SOBRE A VULNERABILIDADE

A vulnerabilidade de **Execução Remota de Código (RCE)** tem origem em uma desserialização insegura de dados não confiáveis, atribuída ao uso inadequado da biblioteca Python *jsonpickle*. Essa falha permite que usuários com privilégios limitados, sem funções de "administrador", realizem a execução de comandos personalizados nos sistemas comprometidos. Conforme a mantenedora, os produtos impactados pela vulnerabilidade incluem o **Splunk Enterprise**, abrangendo as versões *9.3.1* e anteriores, *9.2.3* e anteriores, além das versões específicas entre *9.1.0* e *9.1.6*, que são amplamente utilizadas por diversas organizações para monitoramento de dados. Além disso, o aplicativo **Splunk Secure Gateway** também está comprometido em versões abaixo de *3.7.13* e *3.4.261*, o que pode afetar diretamente as funcionalidades relacionadas ao acesso remoto e integrações móveis.

3 RECOMENDAÇÕES

A Splunk orientou os usuários a atualizarem para as versões mais recentes e seguras: *9.3.2*, *9.2.4* e *9.1.7* no caso do **Splunk Enterprise**, e *3.7.13* ou *3.4.261* para o aplicativo **Splunk Secure Gateway**. Como medida de mitigação imediata, a empresa recomenda desativar o aplicativo **Splunk Secure Gateway**, especialmente se as funções do **Splunk Mobile**, **Spacebridge** e **Mission Control** não estiverem sendo utilizadas.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Splunk**
- **NVD**
- **GBHackers**

5 AUTORES

- **Rafael de Moura Salomé**

heimdall
security research
A DIVISION OF ISH