



# BOLETIM DE SEGURANÇA

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

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	Sumário Executivo .....	4
2	Informação sobre a vulnerabilidade.....	5
3	Recomendações.....	6
4	Referências .....	7
5	Autores.....	7

## 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