

# BOLETIM DE SEGURANÇA

**CISA inclui vulnerabilidade de injeção de comando do  
BeyondTrust no catálogo KEV**

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	Introdução executiva.....	5
2	Informações sobre a vulnerabilidade .....	6
2.1	Sistemas e produtos afetados .....	6
2.2	Impacto da vulnerabilidade .....	6
3	Recomendações.....	7
4	Referências .....	8
5	Autores.....	8

## LISTA DE FIGURAS

Figura 1 – Vulnerabilidade CVE-2024-12686 no catálogo KEV-CISA..... 5

## 1 INTRODUÇÃO EXECUTIVA


---

A CISA adicionou recentemente ao seu [catálogo KEV](#) uma vulnerabilidade de injeção de comandos no BeyondTrust Privileged Remote Access (PRA) e Remote Support (RS), identificada como [CVE-2024-12686](#). Essa falha, atualmente está em exploração ativa, permite que atacantes com privilégios administrativos executem comandos arbitrários diretamente no sistema operacional do servidor que hospeda a aplicação, comprometendo potencialmente a integridade e a segurança dos sistemas afetados.

BEYONDRUST | PRIVILEGED REMOTE ACCESS (PRA) AND REMOTE SUPPORT (RS)

 [CVE-2024-12686](#) 

**BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) OS Command Injection Vulnerability:** *BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) contain an OS command injection vulnerability that can be exploited by an attacker with existing administrative privileges to upload a malicious file. Successful exploitation of this vulnerability can allow a remote attacker to execute underlying operating system commands within the context of the site user.*

Related CWE: [CWE-78](#) 

Known To Be Used in Ransomware Campaigns? **Unknown**

**Action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-01-13
- **Due Date:** 2025-02-03

Figura 1 – Vulnerabilidade CVE-2024-12686 no catálogo KEV-CISA.

## 2 INFORMAÇÕES SOBRE A VULNERABILIDADE

---

A vulnerabilidade CVE-2024-12686 é classificada como uma falha de injeção de comandos do sistema operacional ([CWE-78](#)). Ela permite que um atacante com privilégios administrativos existentes injete comandos que são executados como um usuário do site. A exploração bem-sucedida dessa falha possibilita a execução remota de comandos no sistema afetado, dentro do contexto dos privilégios do aplicativo comprometido.

### 2.1 SISTEMAS E PRODUTOS AFETADOS

Abaixo destacamos os produtos e versões afetadas pela falha:

- *BeyondTrust Privileged Remote Access (PRA) 24.3.1 e anteriores*
- *BeyondTrust Remote Support (RS) 24.3.1 e anteriores*

### 2.2 IMPACTO DA VULNERABILIDADE

- **Comprometimento da Confidencialidade:** O invasor pode acessar dados sensíveis, resultando em vazamentos de informações confidenciais.
- **Comprometimento da Integridade:** Há possibilidade de modificação ou exclusão de dados críticos, comprometendo a integridade das informações.
- **Comprometimento da Disponibilidade:** O invasor pode executar comandos que afetem a disponibilidade dos serviços, potencialmente causando interrupções ou negação de serviço.

## 3 RECOMENDAÇÕES

---

### Aplicar atualizações

- Instale imediatamente as [atualizações](#) fornecidas pela BeyondTrust para corrigir essa vulnerabilidade, as versões afetadas exigem aplicação urgente de patches para mitigar riscos críticos de exploração.

### Revisar privilégios de usuário

- Assegure-se de que os usuários possuam apenas os privilégios necessários para suas funções, seguindo o princípio do menor privilégio. Isso reduz significativamente o risco de exploração interna.

### Monitorar atividades suspeitas

- Implemente monitoramento contínuo para detectar atividades anômalas que possam indicar tentativas de exploração.

## 4 REFERÊNCIAS

---

- Heimdall by ISH Tecnologia
- [CISA](#)
- [BeyondTrust](#)
- [CVE](#)
- [Cyber Security News](#)

## 5 AUTORES

---

- Rafael Salomé





heimdall  
security research

A DIVISION OF ISH