



BOLETIM DE SEGURANÇA

Ivanti lança atualizações críticas para corrigir vulnerabilidades no CSA e Connect Secure

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

1 SUMÁRIO EXECUTIVO

A [Ivanti](#) disponibilizou atualizações de segurança para corrigir múltiplas falhas críticas em seus produtos **Cloud Services Appliance (CSA)** e **Connect Secure**, que poderiam resultar em escalonamento de privilégios e execução de código mal-intencionado.

2 INFORMAÇÕES SOBRE AS VULNERABILIDADES

Abaixo está o detalhamento das vulnerabilidades, incluindo suas descrições e possíveis impactos:

- **[CVE-2024-11639](#)**: Vulnerabilidade de desvio de autenticação no console web do administrador do Ivanti CSA (antes da versão 5.0.3), permitindo que um invasor remoto não autenticado obtenha acesso administrativo.
- **[CVE-2024-11772](#)**: Injeção de comandos no console web do administrador do Ivanti CSA (antes da versão 5.0.3), permitindo que um invasor autenticado remotamente, com privilégios de administrador, execute código remotamente.
- **[CVE-2024-11773](#)**: Injeção de SQL no console web do administrador do Ivanti CSA (antes da versão 5.0.3), permitindo que um invasor remoto autenticado, com privilégios de administrador, realize consultas SQL arbitrárias.
- **[CVE-2024-11633](#)**: Injeção de argumento no Ivanti Connect Secure (antes da versão 22.7R2.4), permitindo execução remota de código por um invasor autenticado com privilégios de administrador.
- **[CVE-2024-11634](#)**: Injeção de comandos no Ivanti Connect Secure (antes da versão 22.7R2.3) e no Ivanti Policy Secure (antes da versão 22.7R1.2), possibilitando a execução remota de código por um invasor autenticado com privilégios de administrador.
- **[CVE-2024-8540](#)**: Vulnerabilidade de permissões inseguras no Ivanti Sentry (antes das versões 9.20.2, 10.0.2 e 10.1.0), permitindo que um invasor local autenticado modifique componentes sensíveis do aplicativo.

As falhas foram resolvidas nas seguintes atualizações:

- *Ivanti Cloud Services Appliance (CSA): Versão 5.0.3.*
- *Ivanti Connect Secure: Versão 22.7R2.4.*
- *Ivanti Policy Secure: Versão 22.7R1.2.*
- *Ivanti Sentry: Versões 9.20.2, 10.0.2 e 10.1.0.*

3 RECOMENDAÇÕES

Embora a Ivanti tenha afirmado que, até o momento, não há relatos de exploração ativa dessas vulnerabilidades, a empresa alerta para a importância de atualizar os sistemas o mais rápido possível. Histórico de ataques anteriores contra produtos Ivanti, inclusive por grupos patrocinados por estados e ransomware, reforça a necessidade de ações preventivas para evitar possíveis explorações maliciosas.

4 REFERÊNCIAS

- Heimdall *by* ISH Tecnologia
- [Ivanti](#)
- [NVD](#)
- [The Hacker News](#)

5 AUTORES

- Rafael de Moura Salomé

