



# ALERTA DE VULNERABILIDADE

Zero-day do MobileIron – Ivanti

CVE-2023-38035

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.



### [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	Resumo da Vulnerabilidade.....	4
2	Referências.....	5

## 1 RESUMO DA VULNERABILIDADE

---

A empresa Ivanti, fornecedora de software de TI com sede nos EUA veio a alertar os clientes e a comunidade sobre uma vulnerabilidade crítica de desvio de autenticação da **Sentry API** que estaria sendo **explorada em massa**.

A Ivanti Sentry (anteriormente MobileIron Sentry) funciona como um “*gatekeeper*” para servidores ActiveSync corporativos, como Microsoft Exchange Server ou recursos de back-end, como servidores Sharepoint em implantações MobileIron e, também poderia operar com um servidor Kerberos Key Distribution Center Proxy (KKDCP).

A vulnerabilidade descoberta e relatada por pesquisadores da mnemônica da empresa de segurança cibernética, a vulnerabilidade crítica (CVE-2023-38035) permite que invasores não autenticados obtenham acesso a APIs confidenciais de configuração do portal de administração expostas na porta 8443, utilizada pelo MobileIron Configuration Service (MICS).

Vale salientar que isso é possível depois que eles ignoram os controles de autenticação, aproveitando uma configuração Apache HTTPD insuficiente restritiva.

A exploração bem-sucedida permite que eles alterem a configuração, executem comandos do sistema ou gravem arquivos em sistemas que executam as versões 9.18 e anteriores do Ivanti Sentry.

A Ivanti acabou por recomendar aos administradores a não expor o MICS à internet e restringir o acesso às redes internas de gerenciamento, seguindo a empresa: “No momento, estamos cientes apenas de um número limitado de clientes afetados pelo CVE-2023-38035. A vulnerabilidade não afeta outros produtos ou soluções Ivanti, como Ivanti EPMM, MobileIron Cloud ou Ivanti Neurons para MDM”.

De acordo com a empresa, a recomendação é que seja **realizada a atualização para a versão suportada e depois aplicar o script RPM** projetado especificamente para a versão.

No Brasil, de acordo com a pesquisa no Shodan **existem 2 dispositivos expostos publicamente** para a internet que podem estar vulneráveis a referida vulnerabilidade.

## 2 REFERÊNCIAS

---

- Heimdall *by* ISH Tecnologia
- [Publicação](#) da Ivanti sobre a CVE-2023-38035
- [Artigo](#) para apoio da CVE-2023-38035
- [Pesquisa](#) Shodan sobre a CVE-2023-38035



**heimdall**  
security research

A DIVISION OF ISH