BOLETIM DE SEGURANÇA

Ivanti alerta sobre falhas críticas em solução de gerenciamento de dispositivos móveis Avalanche

heimdall
security research
A DIVISION OF ISH

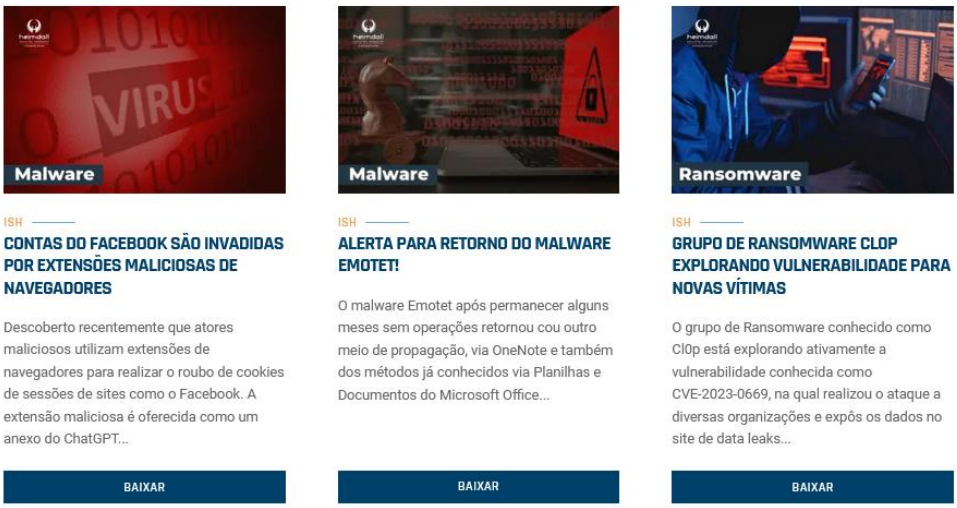
TLP: CLEAR

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

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

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

A Ivanti divulgou a implementação de correções para um total de 27 falhas de segurança identificadas no sistema Avalanche de MDM, destacando-se duas vulnerabilidades críticas de tipo heap overflow que permitem a execução de comandos à distância. O Avalanche é usado utilizado por gestores de TI para controle remoto, distribuição de softwares e programação de updates em extensas coleções de dispositivos móveis, que podem ultrapassar a marca de 100.000 unidades, o Avalanche opera a partir de um ponto centralizado. As vulnerabilidades críticas mencionadas, classificadas como CVE-2024-24996 e CVE-2024-29204, foram detectadas especificamente nos componentes WLInfoRailService e WLAvalancheService, conforme informado pela Ivanti.

2 INFORMAÇÕES SOBRE AS VULNERABILIDADES

A vulnerabilidade CVE-2024-24996, está relacionada a um estouro de heap no componente WLInfoRailService do Ivanti Avalanche antes da versão 6.4.3 permite que um invasor remoto não autenticado execute comandos arbitrários.

A vulnerabilidade CVE-2024-29204, refere-se ao Heap Overflow no componente WLAvalancheService do Ivanti Avalanche antes da versão 6.4.3 permite que um invasor remoto não autenticado execute comandos arbitrários.

Esses ataques são caracterizados pela sua simplicidade e pela ausência de necessidade de interação com o usuário. Além disso, a empresa anunciou a correção de outros 25 bugs de segurança, de gravidade média a alta, que poderiam ser explorados por invasores remotos para provocar ataques de negação de serviço, executar comandos com privilégios de SYSTEM, acessar dados sensíveis na memória e realizar execução remota de código. A empresa assegura que, até o momento da divulgação pública, não há registros de clientes afetados por essas vulnerabilidades. A descoberta dessas falhas ocorreu através do programa de divulgação responsável pela própria Ivanti.

Os sistemas MDM são focos de interesse para agentes de ameaças devido ao seu acesso amplo a dispositivos móveis em larga escala. Uma vulnerabilidade no MobileIron já foi explorada por atores APT, conforme advertência da CISA em agosto de 2023. A exploração dessa brecha preocupa tanto a CISA quanto a NCSC-NO, dada a possibilidade de ataques extensivos em redes do governo e empresas privadas.

Figura 1 – Portais de usuários MobileIron expostos na Internet (Shodan).

3 RECOMENDAÇÕES

Conforme informado pela Ivanti, os usuários podem baixar a versão mais recente do Avalanche 6.4.3 aqui. Para obter informações adicionais sobre as etapas de atualização, consulte este artigo.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Ivanti
- Bleepingcomputer
- NVD

heimdall
security research
A DIVISION OF ISH