TLP: CLEAR

BOLETIM DE SEGURANÇA

Falha de autenticação na Hitachi expõe sistemas a invasões remotas

heimdall
security research

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

SUMÁRIO

1 SUMÁRIO EXECUTIVO

Foi identificada uma vulnerabilidade de bypass de autenticação nos produtos **Hitachi Infrastructure Analytics Advisor** e **Ops Center Analyzer**, representando um alto risco de segurança para os usuários dessas soluções. Catalogada como **CVE-2024-10205**, a falha foi classificada como "**Crítica**" devido ao seu potencial de permitir ataques que comprometem diretamente a integridade dos sistemas, facilitando a exploração por invasores e possibilitando o acesso não autorizado a dados sensíveis e sistemas corporativos.

2 INFORMAÇÃO SOBRE A VULNERABILIDADE

Essa vulnerabilidade permite que agentes não autorizados contornem os mecanismos de autenticação, comprometendo o sistema e causando interrupção de serviços, o que pode resultar na exposição de informações sensíveis. O problema decorre de um desvio de autorização nos componentes de software, impactando diretamente a confidencialidade, a integridade e a disponibilidade dos sistemas afetados.

As versões impactadas variam de acordo com o produto. No caso do **Hitachi Ops Center Analyzer**, o componente vulnerável é o **Analyzer Detail View**, com versões afetadas que vão de *10.0.0-00* até antes de *11.0.3-00*, executadas na plataforma Linux (x64). Já no **Hitachi Infrastructure Analytics Advisor**, o problema está no componente **Data Center Analytics**, abrangendo versões de *2.1.0-00* até *4.4.0-00*, também em Linux (x64).

3 RECOMENDAÇÕES

Para mitigar o risco, a Hitachi disponibilizou versões atualizadas dos produtos, e recomenda-se que os usuários apliquem as correções imediatamente:

- **Hitachi Ops Center Analyzer**: Atualizar para a versão *11.0.3-00* (Linux x64).
- **Hitachi Infrastructure Analytics Advisor**: Contatar a equipe de suporte da Hitachi para obter a versão corrigida mais recente.

Não existem soluções alternativas para contornar o problema. A aplicação das versões corrigidas é a única forma eficaz de proteger os sistemas contra essa vulnerabilidade.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Hitachi**
- **NVD**
- **GBHackers**

5 AUTORES

- **Rafael de Moura Salomé**

heimdall
security research
A DIVISION OF ISH