BOLETIM DE SEGURANÇA

Falha crítica no Veeam Backup Enterprise Manager possibilita a evasão de autenticação

heimdall
security research
A DIVISION OF ISH

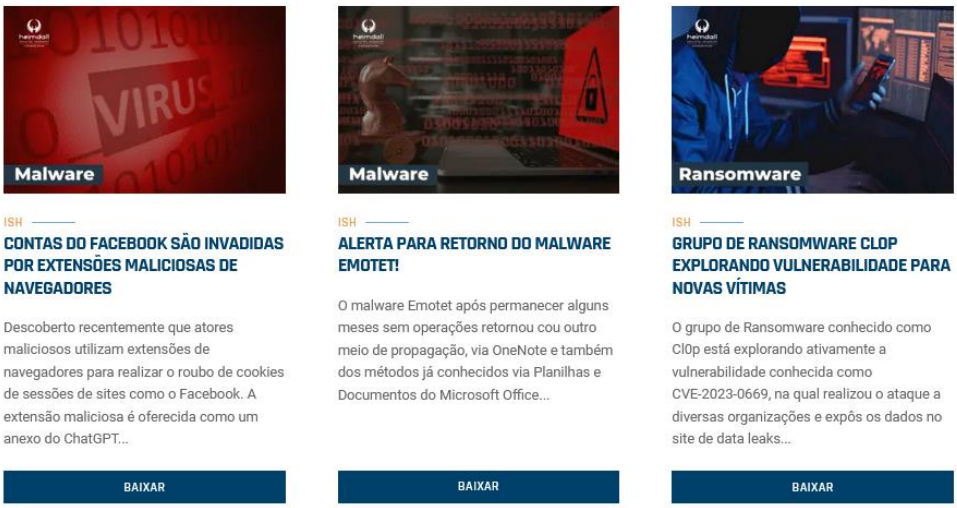
TLP: CLEAR

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

1 SUMÁRIO EXECUTIVO

Foi identificada uma vulnerabilidade CVE-2024-29849 de segurança classificada como crítica no **Veeam Backup Enterprise Manager** que pode permitir a um invasor contornar os mecanismos de autenticação.

2 INFORMAÇÕES SOBRE A VULNERABILIDADE

A vulnerabilidade identificada como CVE-2024-29849 e com uma pontuação CVSS de 9,8, é uma falha de segurança que possibilita um invasor não autenticado acessar a interface web do Veeam Backup Enterprise Manager utilizando as credenciais de qualquer usuário. Esta vulnerabilidade representa um risco significativo e requer atenção imediata.

A empresa divulgou também outras três vulnerabilidades adicionais que impactam o mesmo produto:

- CVE-2024-29850 que possibilita a tomada de controle de uma conta através da retransmissão NTLM.
- CVE-2024-29851, que permite a um usuário com privilégios roubar hashes NTLM de uma conta de serviço do Veeam Backup Enterprise Manager, caso ela não esteja configurada para ser executada como a conta padrão do Sistema Local.
- CVE-2024-29852, que permite a um usuário com privilégios acessar logs de sessão de backup.

Essas falhas foram corrigidas na versão 12.1.2.172 do produto. Contudo, a Veeam ressalta que a instalação do Veeam Backup Enterprise Manager é opcional e, portanto, os ambientes que não o têm instalado não são afetados por essas vulnerabilidades

Também houve correções nas vulnerabilidades CVE-2024-29853 de escalonamento de privilégios locais que impactava o Veeam Agent for Windows, vulnerabilidade CVE-2024-29212 categorizada como crítica, pois trata-se de execução remota de código que afetava o Veeam Service Provider, que ocorre devido a um método de desserialização inseguro empregado pelo servidor Veeam Service Provider Console (VSPC) na comunicação entre o agente de gerenciamento e seus componentes. Sob determinadas condições, isso possibilita a execução remota de código (RCE) na máquina do servidor VSPC.

A vulnerabilidades CVE-2023-27532 de segurança no software Veeam Backup & Replication foram exploradas por agentes de ameaças, como FIN7 e Cuba, para implantar cargas maliciosas, incluindo ransomware. Portanto, é crucial que os usuários corrijam rapidamente as vulnerabilidades citadas.

3 RECOMENDAÇÕES

A Empresa recomenda que os usuários do Veeam Backup Enterprise Manager atualizem a para a versão mais recente após a descoberta de uma falha crítica de segurança.

- **Atualização**: Atualize para a versão 12.1.2.172 do Veeam Backup Enterprise Manager, que aborda a CVE-2024-29849. Esta atualização corrige a falha que poderia permitir que um adversário contornasse as proteções de autenticação.
- **Mitigação de Vulnerabilidade**: Caso não seja possível atualizar imediatamente o Veeam Backup Enterprise Manager para a versão 12.1.2.172, considere interromper o software Veeam Backup Enterprise Manager. Para fazer isso, pare e desative o serviço Veeam Backup Enterprise Manager.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Veeam
- Csirt_Morenet
- Thehackernews

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH