BOLETIM DE SEGURANÇA

Falha crítica no Cellopoint Secure Email Gateway permitindo execução remota de código

heimdall
security research
A DIVISION OF ISH

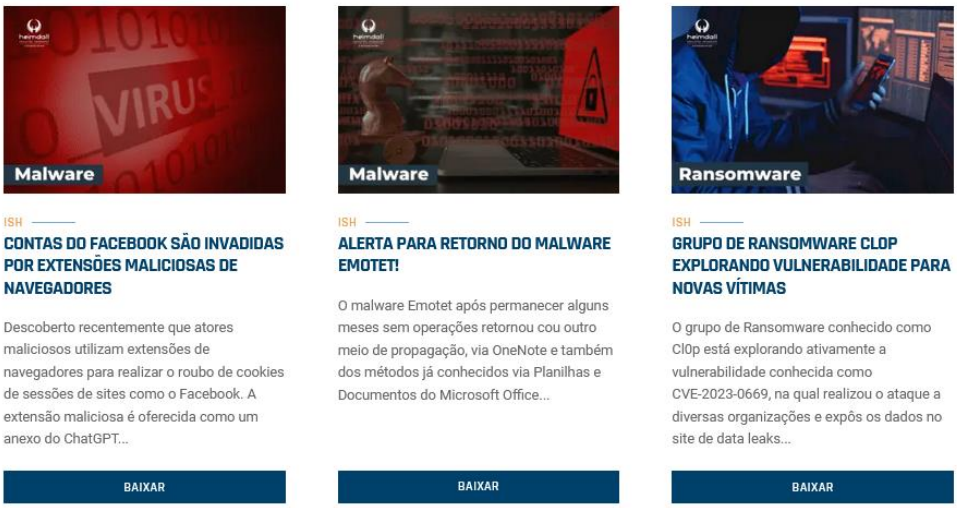
TLP: CLEAR

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

Foi identificada uma falha crítica, **CVE-2024-6744**, no Cellopoint Secure Email Gateway. Esta vulnerabilidade, que recebeu uma pontuação CVSS de 9,8, representa uma ameaça significativa para as organizações que utilizam este sistema de segurança de e-mail.

2 INFORMAÇÕES SOBRE A VULNERABILIDADE

O relatório da Twcert revelou a existência da vulnerabilidade CVE-2024-6744 no componente SMTP Listener do Secure Email Gateway, especificamente em versões anteriores à 4.5.0. A falha é resultado de uma validação inadequada da entrada do usuário, o que leva a um estouro de buffer.

Esta vulnerabilidade permite que um invasor remoto não autenticado execute comandos arbitrários no servidor afetado, colocando em risco potencial toda a infraestrutura de e-mail.

Identificação da TVN	TVN-202407010
Identificação CVE	CVE-2024-6744
CVSS	9.8 (Crítico) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Produtos afetados	Secure Email Gateway antes da versão 4.5.0
Descrição	O SMTP Listener do Secure Email Gateway da Cellopoint não valida corretamente a entrada do usuário, levando a uma vulnerabilidade de Buffer Overflow. Um invasor remoto não autenticado pode explorar essa vulnerabilidade para executar comandos de sistema arbitrários no servidor remoto.
Solução	Instale o patch Build_20240529 ou posterior
Crédito	Ponto de violoncelo
Data Pública	2024-07-15

Figura 1 – Detalhes técnicos.

Em resposta a esta questão crítica, a Cellopoint lançou prontamente um patch, Build_20240529, que resolve a vulnerabilidade. É imperativo que todas as organizações que utilizam as versões afetadas do Secure Email Gateway instalem este patch imediatamente para minimizar o risco de exploração.

A descoberta do CVE-2024-6744 destaca os desafios contínuos na proteção dos gateways de e-mail, que são componentes vitais da infraestrutura de comunicação empresarial. A capacidade de um invasor executar código arbitrário remotamente sem autenticação destaca a importância de atualizações de segurança regulares e monitoramento atento. A Cellopoint foi reconhecida por identificar e tratar esta vulnerabilidade.

A divulgação pública desta falha em 15 de julho de 2024 tem como objetivo garantir que todos os usuários afetados estejam cientes e possam tomar as medidas necessárias para proteger seus sistemas.

3 RECOMENDAÇÕES

Identificação de sistemas vulneráveis

- Identifique os sistemas Microsoft Outlook vulneráveis sob sua responsabilidade e aplique as devidas atualizações.

Bloqueio de tráfego

- Até que as atualizações sejam instaladas, recomenda-se, como medida de mitigação, o bloqueio do tráfego da porta 445/SMB para fora da rede, de modo a impedir o envio de mensagens de autenticação NTLM.

Utilização de grupo de usuários protegidos

- Recomenda-se a utilização do recurso de grupo de usuários protegidos do Active Directory para as contas dos administradores de domínio.

Monitoramento de tentativas de exploração

- Utilize regras de firewall e sistemas de detecção/prevenção de intrusões (IDS/IPS) para monitorar e bloquear tentativas de exploração desta vulnerabilidade.

Proteção de dados pessoais

- Proteja seus dados pessoais contra roubo e acessos não autorizados.

Detecção e remoção de ameaças cibernéticas

- Detecte e remova ameaças cibernéticas em tempo real.

4 REFERÊNCIAS

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

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH