BOLETIM DE SEGURANÇA

CVE-2024-4040, Vulnerabilidade crítica no CrushFTP sendo explorada em ataques

heimdall
security research
A DIVISION OF ISH

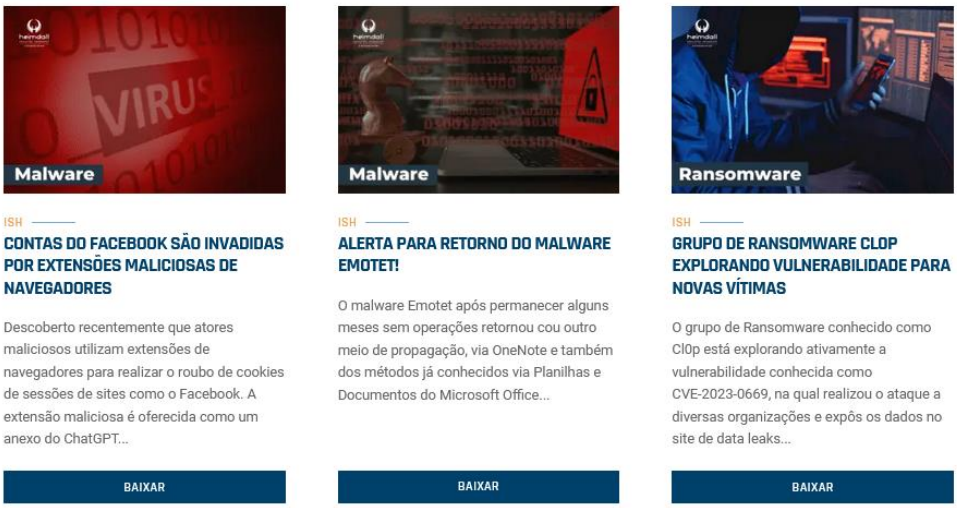
TLP: CLEAR

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

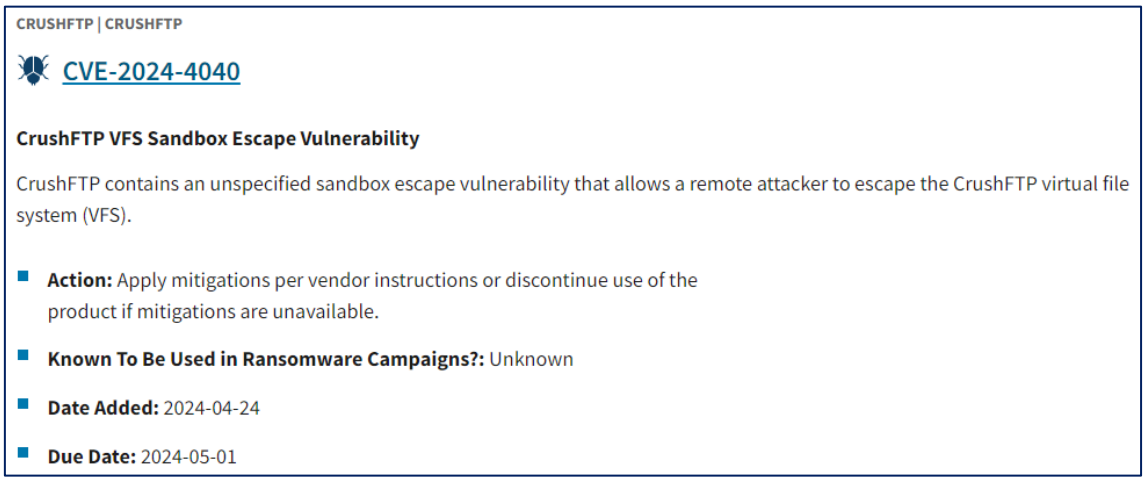


SUMÁRIO

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Recentemente a *Cybersecurity and Infrastructure Security Agency* (CISA), adicionou em seu catalogo de vulnerabilidades conhecida (KEV), a falha critica CVE-2024-4040 no CrushFTP, a qual vem sendo explorada em ataques cibernéticos.



CRUSHFTP | CRUSHFTP

CVE-2024-4040

CrushFTP VFS Sandbox Escape Vulnerability

CrushFTP contains an unspecified sandbox escape vulnerability that allows a remote attacker to escape the CrushFTP virtual file system (VFS).

- **Action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
- **Known To Be Used in Ransomware Campaigns?:** Unknown
- **Date Added:** 2024-04-24
- **Due Date:** 2024-05-01

Figura 1 – Vulnerabilidade no catálogo KEV-CISA.

2 DETALHES SOBRE A VULNERABILIDADE

A vulnerabilidade CVE-2024-4040 no CrushFTP é uma falha crítica que permite a um atacante com privilégios baixos escapar do sandbox do sistema de arquivos virtual (VFS) e acessar arquivos do sistema fora deste ambiente restrito. A vulnerabilidade, descrita como uma falha de validação de entrada, afeta todas as versões do CrushFTP anteriores às 10.7.1 e 11.1.0 em todas as plataformas. A exploração bem-sucedida dessa vulnerabilidade pode permitir a leitura de arquivos de sistema, potencialmente levando a uma escalada de privilégios e execução remota de código.

Esse problema foi explorado ativamente antes que correções estivessem disponíveis, e ataques direcionados foram observados, especialmente em entidades nos EUA, com indícios de que os ataques possam ter motivações políticas para coleta de inteligência. Os atacantes têm como alvo servidores vulneráveis do CrushFTP para roubar informações confidenciais e realizar outras atividades maliciosas.

Anteriormente, relatórios sugeriam que se o CrushFTP estivesse atrás de uma zona desmilitarizada (DMZ) , os usuários estariam protegidos contra essa falha. No entanto, a partir de 22 de abril, o CrushFTP contestou esta afirmação, observando que uma DMZ “não protege você totalmente”. Os clientes que usam uma versão vulnerável do CrushFTP são aconselhados a atualizar para uma versão corrigida o mais rápido possível.

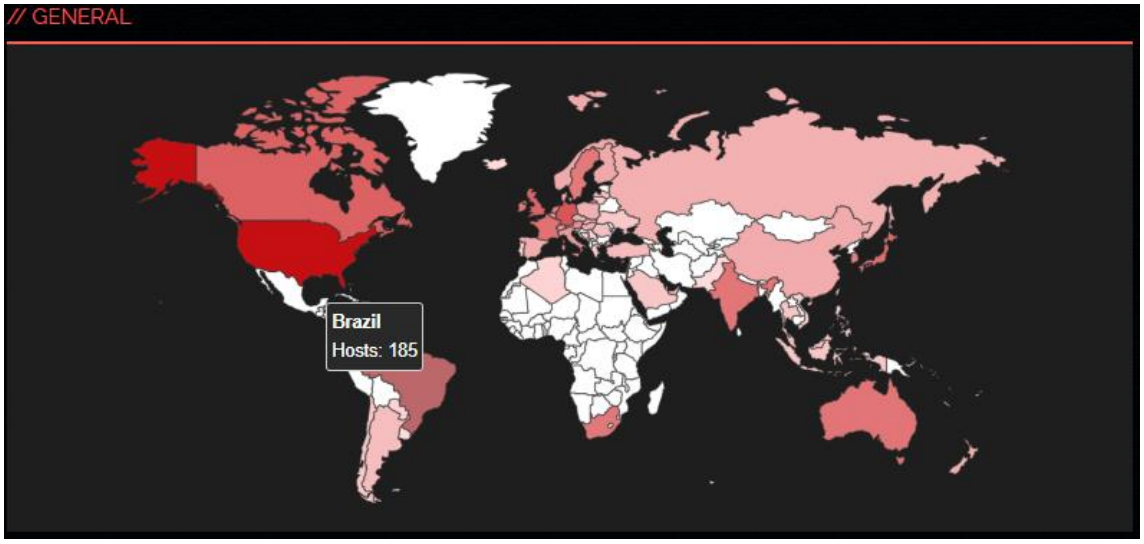


Figura 2 – Servidores CrushFTP expostos online.

Em uma pesquisa realizada pela ferramenta Shodan.io, é possível observar milhares de servidores CrushFTP expostos online e potencialmente vulneráveis. É notável também que 185 desses servidores estão em organizações no brasil, o que mesmo não sendo uma grande quantidade, acarreta riscos de segurança para estas organizações.

3 CONCLUSÃO

A exploração da vulnerabilidade no CrushFTP representa sérios riscos para organizações. Permitindo que atacantes escapem do sandbox do sistema de arquivos virtual, essa falha pode resultar no acesso não autorizado a arquivos confidenciais do sistema, comprometendo a integridade e a confidencialidade dos dados corporativos. O risco se estende à possibilidade de execução de código remoto, aumentando o potencial de danos e permitindo aos atacantes assumir o controle total dos sistemas afetados. Além disso, ataques bem-sucedidos podem facilitar atividades maliciosas adicionais, como espionagem, roubo de dados e disseminação de malware. As organizações devem atualizar rapidamente seus sistemas para as versões seguras do software, a fim de mitigar esses riscos e proteger suas infraestruturas críticas.

4 RECOMENDAÇÕES

A CrushFTP já lançou patches de correção para as versões 10 e 11 do software, e recomenda-se que os usuários atualizem seus sistemas o mais rápido possível para evitar a exploração da vulnerabilidade.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Tenable
- CISA-KEV
- NVD
- CrushFTP

heimdall
security research
A DIVISION OF ISH