BOLETIM DE SEGURANÇA

Vulnerabilidade do Sharepoint, adicionada ao catálogo KEV da CISA

heimdall
security research
A DIVISION OF ISH

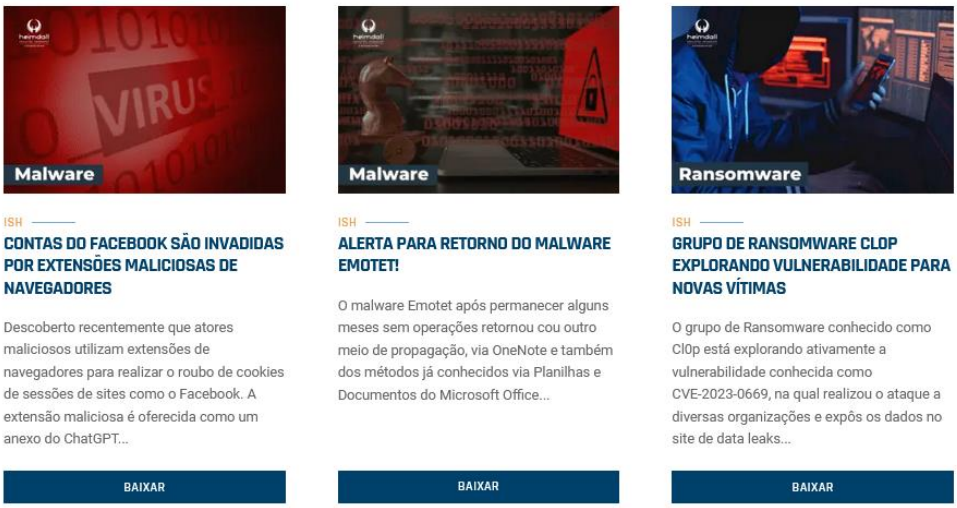
TLP: CLEAR

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 Agência de Segurança Cibernética (**CISA**) incluiu no seu catálogo de vulnerabilidades uma falha de segurança que afeta o Microsoft Sharepoint Server. Essa vulnerabilidade, rastreada como CVE-2023-24955, é uma falha de *remote code execution* (**RCE**). Ela permite que um invasor autenticado com privilégios de proprietário do site execute código arbitrário. Em um ataque baseado em rede, um invasor autenticado como proprietário do site poderia executar código remotamente no servidor SharePoint. Dois meses antes, foi incluída a CVE-2023-29357, categorizada como crítica, tratando-se de uma falha de *privilege escalation* no SharePoint Server.

2 DETALHES SOBRE A VULNERABILIDADE

A CVE-2023-24955 é uma vulnerabilidade RCE que afeta o Microsoft SharePoint Server. A vulnerabilidade pode permitir que um proprietário de site autenticado execute código em um servidor SharePoint afetado. Este RCE foi corrigido como parte do lançamento do Patch Tuesday de maio de 2023.

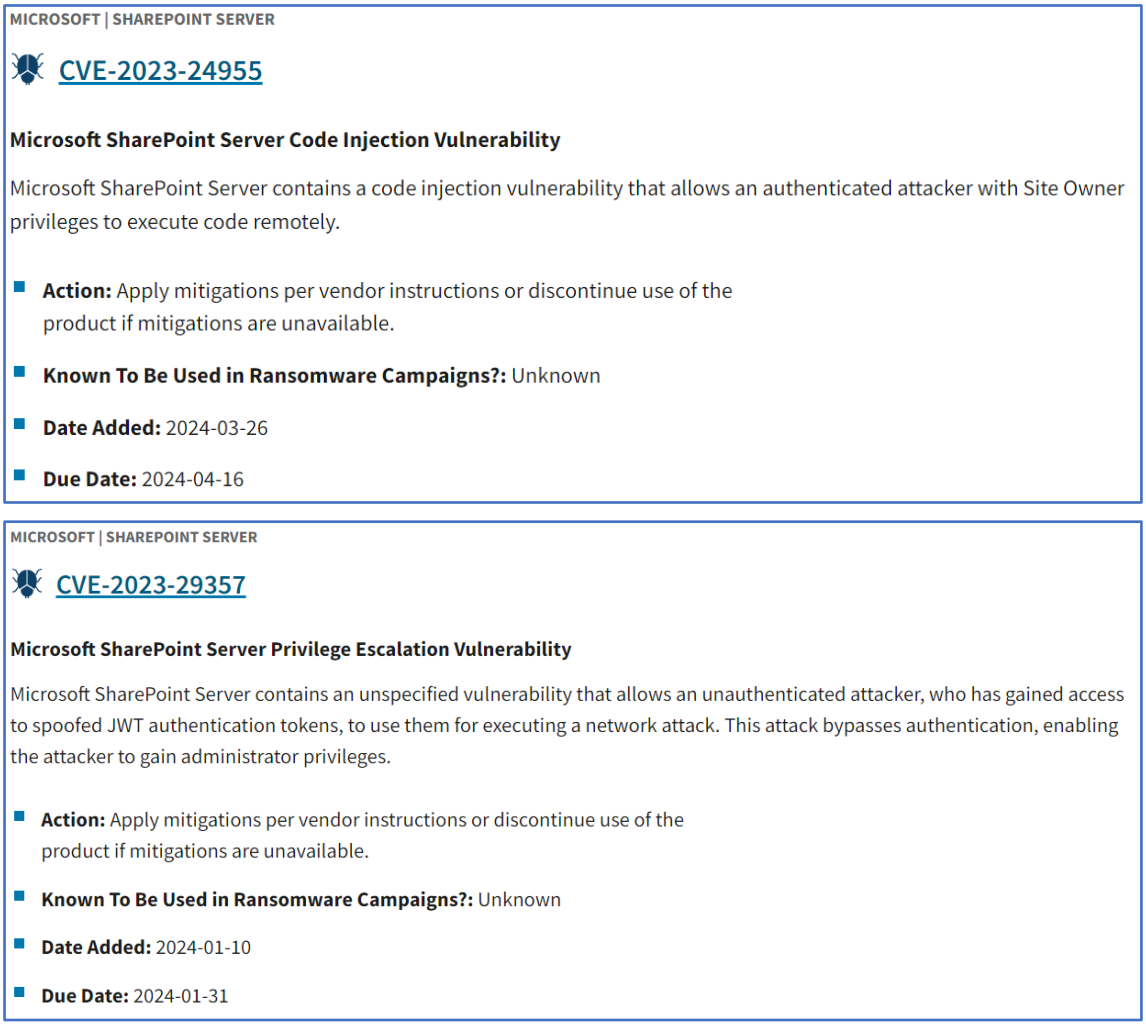
Atualmente não há informações sobre os ataques que usam essa vulnerabilidade como arma e os atores da ameaça que podem estar explorando-a.

Mitigações

- É necessário **atualizar** para as **versões mais recentes** como mostra na tabela acessando o link.

3 VULNERABILIDADES NO CATÁLOGO KEV-CISA

A agência de segurança cibernética (CISA) adicionou as falhas ao seu Catálogo de Vulnerabilidades Exploradas Conhecidas (KEV), dizendo que tais vulnerabilidades são “vetores de ataque frequentes para atores cibernéticos maliciosos”.



MICROSOFT | SHAREPOINT SERVER

CVE-2023-24955

Microsoft SharePoint Server Code Injection Vulnerability

Microsoft SharePoint Server contains a code injection vulnerability that allows an authenticated attacker with Site Owner privileges to execute code remotely.

- **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:** 2024-03-26
- **Due Date:** 2024-04-16

MICROSOFT | SHAREPOINT SERVER

CVE-2023-29357

Microsoft SharePoint Server Privilege Escalation Vulnerability

Microsoft SharePoint Server contains an unspecified vulnerability that allows an unauthenticated attacker, who has gained access to spoofed JWT authentication tokens, to use them for executing a network attack. This attack bypasses authentication, enabling the attacker to gain administrator privileges.

- **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:** 2024-01-10
- **Due Date:** 2024-01-31

Figura 1 – Vulnerabilidades no catálogo KEV-CISA.

4 RECOMENDAÇÕES

São elencados abaixo pela ISH, medidas que poderão ser adotadas visando a exploração das referidas *vulnerabilidades*, como por exemplo:

CVE-2023-24955

- Aplicar patches: Aplique os patches de segurança emitidos pela Microsoft para mitigar a vulnerabilidade.
- Atualizar o SharePoint: Certifique-se de que o SharePoint Server esteja atualizado com a versão mais recente.
- Monitoramento contínuo: Considere usar uma plataforma de análise comportamental de endpoints para receber alertas em tempo real e bloquear ameaças potenciais.

CVE-2023-29357

- Aplicar patches: Aplique os patches de segurança emitidos pela Microsoft para proteger seus servidores vulneráveis.
- Atualizar o SharePoint: Certifique-se de que o SharePoint Server esteja atualizado o mais rápido possível.
- Monitoramento proativo: Considere usar uma plataforma de segurança como o Barracuda XDR para análise comportamental contínua e bloqueio de ameaças.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Thehackernews
- NVD
- CISA-KEV

heimdall
security research
A DIVISION OF ISH