BOLETIM DE SEGURANÇA

Falha crítica na infraestrutura cibernética da Acronis sendo explorada em ataques

heimdall
security research
A DIVISION OF ISH

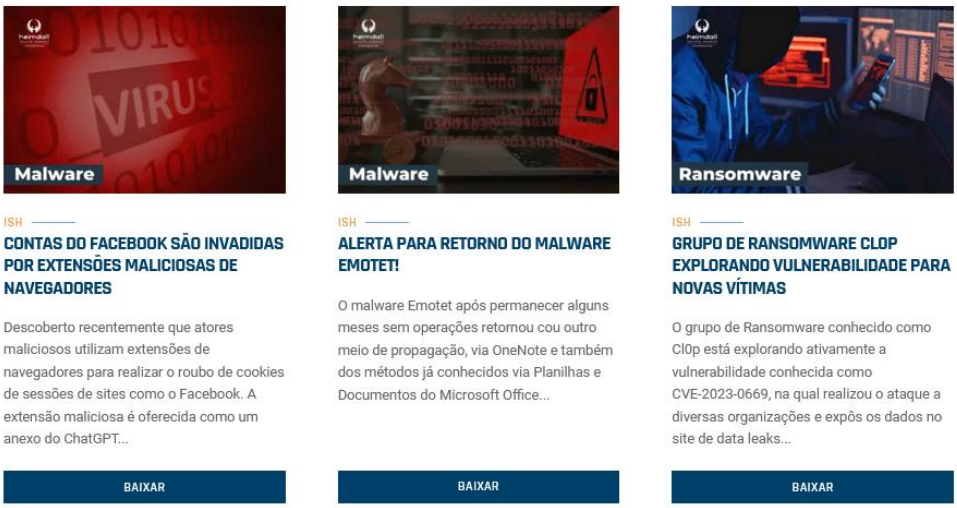
TLP: CLEAR

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

A Acronis emitiu um alerta para que os clientes corrijam uma vulnerabilidade crítica na infraestrutura cibernética, **CVE-2023-45249** (pontuação CVSS: 9,8), a qual possibilita que invasores contornem a autenticação em servidores vulneráveis usando credenciais padrão. Esse problema já foi explorado em ataques, e a Acronis aconselhou os administradores a atualizarem suas instalações o mais rápido possível. A Acronis Cyber Infrastructure (ACI) é uma plataforma unificada multi-tenant para proteção cibernética, que integra funcionalidades de gerenciamento remoto de endpoints, backup e virtualização. Além disso, a ACI é projetada para executar tarefas de recuperação de desastres e armazenar de forma segura os dados de backup corporativos.

Figura 1 – Dispositivos Acronis expostos na Internet-Top 05 países.

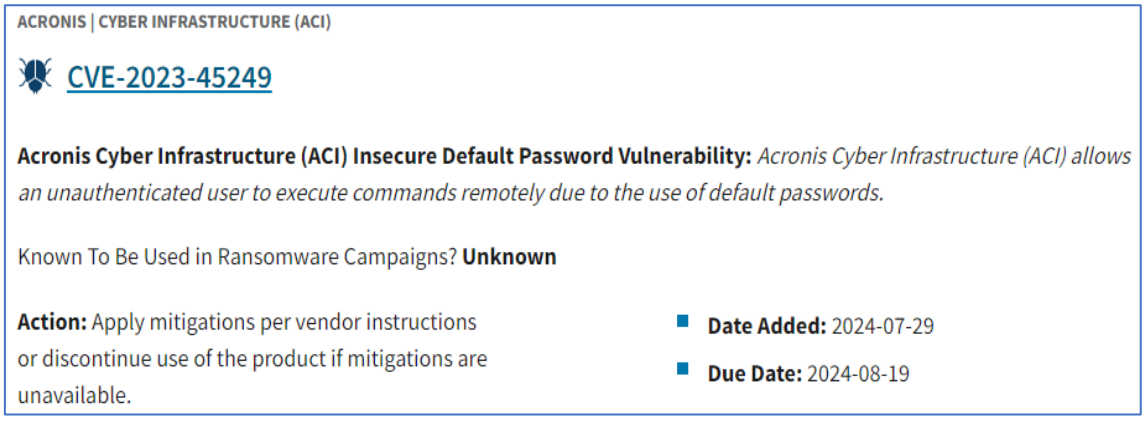
2 INFORMAÇÕES SOBRE A VULNERABILIDADE

Como mencionado anteriormente, a vulnerabilidade é rastreada como CVE-2023-45249 (pontuação CVSS: 9,8), diz respeito a um caso de execução remota de código decorrente do uso de senhas padrão e afeta as seguintes versões do Acronis Cyber Infrastructure (ACI):

- *Acronis Cyber Infrastructure (ACI) antes da build 5.0.1-61 (**corrigido na atualização 1.4 do ACI 5.0**),*
- *Acronis Cyber Infrastructure (ACI) antes da build 5.1.1-71 (**corrigido na atualização 1.2 do ACI 5.1**),*
- *Acronis Cyber Infrastructure (ACI) antes da build 5.2.1-69 (**corrigido na atualização 1.3 do ACI 5.2**),*
- *Acronis Cyber Infrastructure (ACI) antes da build 5.3.1-53 (**corrigido na atualização 1.3 do ACI 5.3**),*
- *Acronis Cyber Infrastructure (ACI) antes da build 5.4.4-132 (**corrigido na atualização 4.2 do ACI 5.4**).*

3 VULNERABILIDADE ADICIONADA AO KEV-CISA

Devido estas explorações a vulnerabilidade já foi adicionada ao Catálogo de Vulnerabilidades Exploradas Conhecidas (KEV).


ACRONIS | CYBER INFRASTRUCTURE (ACI)

CVE-2023-45249

Acronis Cyber Infrastructure (ACI) Insecure Default Password Vulnerability: *Acronis Cyber Infrastructure (ACI) allows an unauthenticated user to execute commands remotely due to the use of default passwords.*

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2024-07-29
- **Due Date:** 2024-08-19

Figura 2 – Falha no catálogo da CISA-KEV.

4 CONCLUSÃO

A falha de segurança CVE-2023-45249 no Acronis representa um risco significativo, pois pode ser explorada por atores maliciosos para comprometer sistemas críticos. Esta vulnerabilidade permite a execução remota de código, proporcionando aos invasores a capacidade de assumir o controle total dos sistemas afetados. Organizações que utilizam o Acronis estão particularmente em risco, pois os dados protegidos por esta ferramenta podem ser acessados e manipulados indevidamente. A exploração desta falha pode levar ao roubo de informações sensíveis, interrupção de serviços e disseminação de malware. A sofisticação dos ataques aumenta o desafio de detecção e resposta. É crucial que as organizações atualizem seus sistemas e implementem medidas de segurança adicionais para mitigar este risco.

5 RECOMENDAÇÕES

Atualização da falha conforme recomendação do fabricante.

Para verificar se seus servidores estão vulneráveis, você pode encontrar o número da compilação do Acronis Cyber Infrastructure acessando a caixa de diálogo *Help -> About* na janela principal do software.

Para atualizar o ACI para a versão mais recente disponível, você precisa:

- Entre na sua conta (você pode criar uma e registrar suas licenças usando estas instruções).
- Baixe a versão mais recente do ACI na seção "Products" e instale-a em servidores vulneráveis.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Acronis
- Bleepingcomputer
- NVD
- KEV-CISA

7 AUTORES

- **Ismael Rocha**

heimdall
security research
A DIVISION OF ISH