TLP: CLEAR

# ALERTA DE SEGURANÇA

## Falha em arquivo da Crowdstrike causa interrupções em serviços Windows

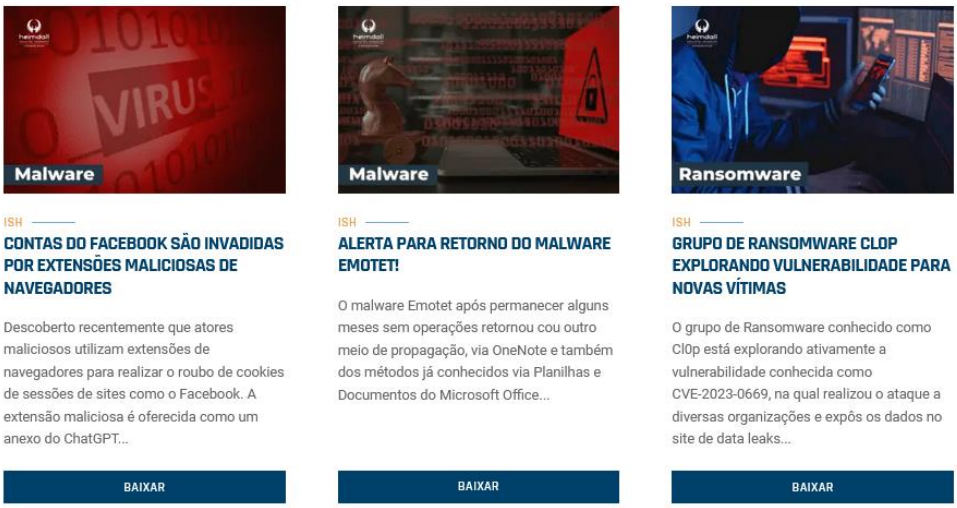
heimdall
security research
A DIVISION OF ISH

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 TABELAS

## LISTA DE FIGURAS

# 1 SUMÁRIO EXECUTIVO

Na última noite (18), a empresa de segurança de endpoint **Crowdstrike** lançou uma atualização que está causando “telas azuis da morte” (BSOD) generalizadas em sistemas Windows.

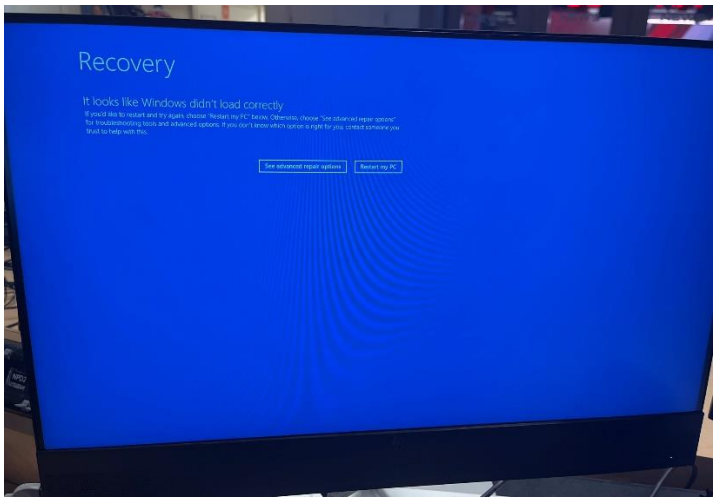



*Figura 1 – Tela azul da Morte (BSOD) apresentada nos dispositivos.*


*Figura 2 – Tela azul da Morte (BSOD) apresentada nos dispositivos.*

A Crowdstrike publicou um comunicado que só está disponível após fazer o login na plataforma de suporte, onde também há uma breve declaração pública sobre o tema. De acordo com a avaliação e coleta das informações, apenas os sistemas Windows são afetados e teria sido ocasionado por um arquivo utilizado na estrutura.

Foram fornecidas suporte para mitigar até que o driver e toda a infraestrutura do serviço seja retornada ao seu normal, portando, é recomendado que as empresas realizem a seguinte ação:

1. Inicialize o Windows no **modo de segurança** ou no **ambiente de recuperação**.
2. Navegue até o diretório **“C:\Windows\System32\drivers\CrowdStrike”.**
3. Localize o arquivo correspondente a **“C-00000291*.sys”** e exclua-o.

```
del "C:\Windows\System32\drivers\CrowdStrike\C-00000291*.sys"
```

4**. Inicialize o host normalmente**.

Acrescentamos ainda que não é a primeira vez que um software de segurança causa falhas nos sistemas. Isso pode ocorrer devido aos sistemas de segurança marcarem alguns arquivos como falsos positivos, categorizando-os como maliciosos e agindo contra eles, o que pode ocasionar falhas como as vistas hoje.

## 2 SERVIÇOS AFETADOS

É válido salientar que o problema ocasionou falhas de longo alcance, afetando aeroportos, sistemas de polícias, bancos e diversos outros setores de acordo com a coleta de informações realizadas pelo time de Inteligência:

| País | Categoria | Detalhes |
|---|---|---|
| **Austrália** | Mídia | ABC, SBS, Seven Network, Nine Network |
| **Austrália** | Companhias Aéreas | Qantas, Virgin Australia, Jetstar |
| **Austrália** | Aeroportos | Sydney, Melbourne |
| **Austrália** | Supermercados | Woolworths, Coles |
| **Austrália** | Bancos | NAB, ANZ, Commonwealth Bank, Bendigo Bank, Suncorp |
| **Austrália** | Varejistas e Fast Food | KFC, sistemas de autoatendimento |
| **Canadá** | Bancos | TD Canada Trust interrupção no aplicativo móvel |
| **Bélgica** | Serviços de Trem | Compras de bilhetes de trem, anúncios digitais |
| **Bélgica** | Mídia | JOE, QMusic |
| **Bélgica** | Bancos e Serviços Postais | |
| **Bélgica** | Aeroportos | Bruxelas, Charleroi |
| **França** | Canais de TV | TF1, TFX, LCI, Canal+ |
| **França** | Sistemas | Sistemas para os Jogos Olímpicos de Paris 2024 |
| **Croácia** | Saúde e Tráfego Aéreo | Sistema Central de Informações de Saúde, Controle de Tráfego Aéreo |
| **Alemanha** | Aeroportos e Companhias Aéreas | Aeroporto de Berlim, Lufthansa |
| **Alemanha** | Hospitais | Hospitais em Lübeck e Kiel |
| **Hong Kong SAR** | Aeroportos | Aeroporto Internacional de Hong Kong |
| **Hong Kong SAR** | Companhias Aéreas | Cathay Pacific, Hong Kong Express, Hong Kong Airlines |
| **Índia** | Companhias Aéreas | Air India, Indigo, Akasa Air, SpiceJet, Vistara |
| **Índia** | Empresas de TI | Oracle, Nokia |
| **Israel** | Emergência e Saúde | Magen David Adom, Hospitais: Sheba, Laniado, Rambam |
| **Israel** | Serviços | Israel Post, bancos, empresas farmacêuticas |
| **Malásia** | Serviços Ferroviários | Sistema de bilhetagem do operador ferroviário KTMB |
| **Países Baixos** | Aeroportos e Companhias Aéreas | Aeroporto Schiphol, Transavia Airlines |
| **Países Baixos** | Bancos | Banco KNAB |

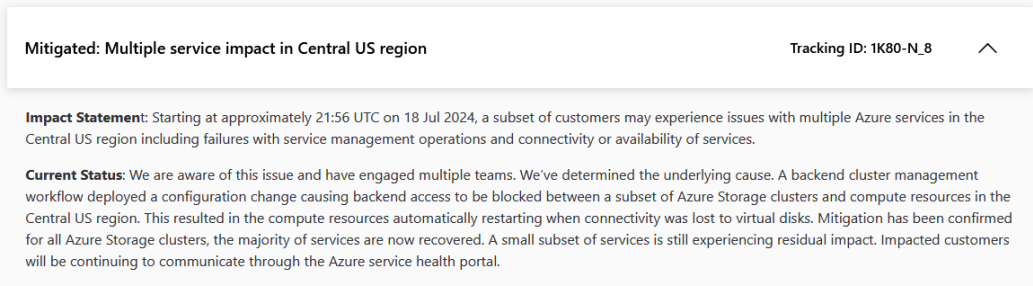
| | | |
|---|---|---|
| **Países Baixos** | Serviços Governamentais | Serviços governamentais, hospitais |
| **Nova Zelândia** | Bancos | ANZ, ASB, Kiwibank, Westpac |
| **Nova Zelândia** | Supermercados | Woolworths, Foodstuffs |
| **Nova Zelândia** | Transporte e Aeroportos | Auckland Transport, Aeroporto de Christchurch |
| **Filipinas** | Vários Serviços | Bancos, telecomunicações, transmissões, supermercados |
| **Filipinas** | Companhias Aéreas | Voos da Cebu Pacific |
| **Coreia do Sul** | Companhias Aéreas | Jeju Air |
| **Singapura** | Aeroportos | Aeroporto Changi |
| **Espanha** | Serviços de Navegação Aérea | Aena da ENAIRE |
| **Suíça** | Aeroportos | Aeroporto de Zurique |
| **Reino Unido** | Mídia | Sky News, CBBC |
| **Reino Unido** | Aeroportos | Aeroportos de Edimburgo e Gatwick |
| **Reino Unido** | Empresas Ferroviárias | |
| **Reino Unido** | Serviços de Saúde | Serviços do NHS |
| **Reino Unido** | Serviços Financeiros | Bolsa de Valores de Londres |
| **Reino Unido** | Varejistas | Ladbrokes Coral |
| **Estados Unidos** | Companhias Aéreas | Interrupções de voos para United, Delta, American Airlines |
| **Estados Unidos** | Serviços de Emergência | Interrupções no serviço 911 em Alaska, Arizona, New Hampshire |

Tabela 1 – Exemplo de serviços paralisados.

# 3 OUTRAS INTERRUPÇÕES

Outra interrupção também ocorreu no serviço da **Microsoft365**, afetando as organizações que utilizam o serviço na região central dos EUA.

De acordo com a Microsoft, alguns dos serviços afetados foram: Microsoft Defender, Intune, Teams, PowerBI, Fabric, OneNote for Business, SharePoint Online, Windows 365, Viva Engage, Microsoft Purview e o centro de administração do Microsoft 365.

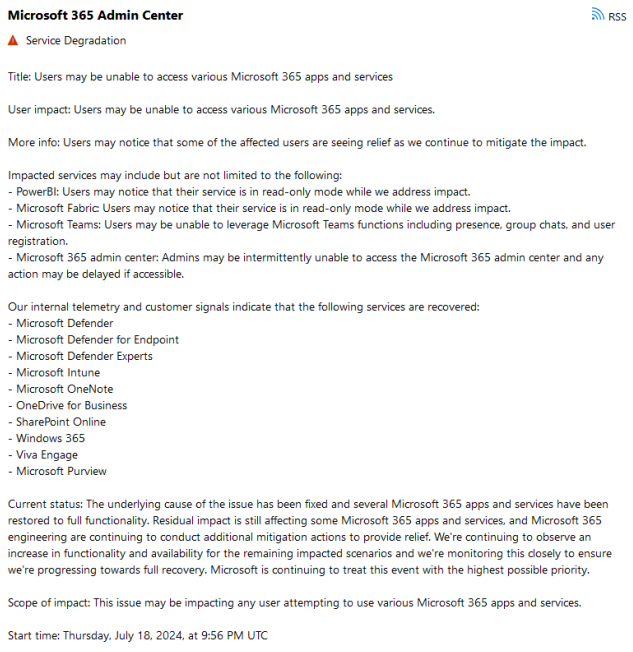


**Mitigated: Multiple service impact in Central US region** Tracking ID: 1K80-N_8

**Impact Statement**: Starting at approximately 21:56 UTC on 18 Jul 2024, a subset of customers may experience issues with multiple Azure services in the Central US region including failures with service management operations and connectivity or availability of services.

**Current Status**: We are aware of this issue and have engaged multiple teams. We've determined the underlying cause. A backend cluster management workflow deployed a configuration change causing backend access to be blocked between a subset of Azure Storage clusters and compute resources in the Central US region. This resulted in the compute resources automatically restarting when connectivity was lost to virtual disks. Mitigation has been confirmed for all Azure Storage clusters, the majority of services are now recovered. A small subset of services is still experiencing residual impact. Impacted customers will be continuing to communicate through the Azure service health portal.

*Figura 3 – Explicação da Microsoft para paralisação dos serviços.*



**Microsoft 365 Admin Center** RSS

Service Degradation

Title: Users may be unable to access various Microsoft 365 apps and services

User impact: Users may be unable to access various Microsoft 365 apps and services.

More info: Users may notice that some of the affected users are seeing relief as we continue to mitigate the impact.

Impacted services may include but are not limited to the following:
- PowerBI: Users may notice that their service is in read-only mode while we address impact.
- Microsoft Fabric: Users may notice that their service is in read-only mode while we address impact.
- Microsoft Teams: Users may be unable to leverage Microsoft Teams functions including presence, group chats, and user registration.
- Microsoft 365 admin center: Admins may be intermittently unable to access the Microsoft 365 admin center and any action may be delayed if accessible.

Our internal telemetry and customer signals indicate that the following services are recovered:
- Microsoft Defender
- Microsoft Defender for Endpoint
- Microsoft Defender Experts
- Microsoft Intune
- Microsoft OneNote
- OneDrive for Business
- SharePoint Online
- Windows 365
- Viva Engage
- Microsoft Purview

Current status: The underlying cause of the issue has been fixed and several Microsoft 365 apps and services have been restored to full functionality. Residual impact is still affecting some Microsoft 365 apps and services, and Microsoft 365 engineering are continuing to conduct additional mitigation actions to provide relief. We're continuing to observe an increase in functionality and availability for the remaining impacted scenarios and we're monitoring this closely to ensure we're progressing towards full recovery. Microsoft is continuing to treat this event with the highest possible priority.

Scope of impact: This issue may be impacting any user attempting to use various Microsoft 365 apps and services.

Start time: Thursday, July 18, 2024, at 9:56 PM UTC

*Figura 4 – Aviso da Microsoft para paralisação dos serviços.*

Durante a interrupção, a Microsoft direcionou o o tráfego impactado para sistemas alternativos para aliviar o impacto e, posteriormente, a Microsoft afirmou que o problema foi causado por um fluxo de trabalho de gerenciamento de cluster de back-end ao implementar uma mudança de configuração fazendo com que o acesso de back-end fosse bloqueado entre um subconjunto de clusters de armazenamento do Azure, bem como recursos de computação na região central dos EUA.

# 4 RECOMENDAÇÕES E CONCLUSÃO

Recomendamos que sejam aplicados e utilizados os comandos mencionados acima para fins de mitigação do problema relacionado a Crowdstrike, bem como que seja aguardada a atualização e correção do problema que possivelmente será disponibilizado pela empresa no futuro.

# 5 REFERÊNCIAS


- **Heimdall *by* ISH Tecnologia**

heimdall
security research
A DIVISION OF ISH