Cyber Threat Intelligence

Report

Cyber Threat Intelligence

CTI – Atualização de Patch da CrowdStrike resulta em falhas relacionadas ao Falcon-Sensor

2024 | Document Version 0.01

Table of Contents

1. Introdução

Em 19 de julho de 2024, uma atualização no software de segurança da CrowdStrike resultou em falhas críticas, causando a Tela Azul da Morte (BSOD) em sistemas Windows globalmente. Este incidente afetou milhões de dispositivos, incluindo aqueles de serviços essenciais, destacando a importância de procedimentos rigorosos de teste e validação em atualizações de software. Este documento fornece uma visão geral do ocorrido, os impactos e as medidas corretivas adotadas para mitigar os efeitos do incidente.

2. Descrição do Incidente

A falha foi atribuída a um erro no driver csagent.sys, que gerou um código de parada *PAGE_FAULT_IN_NONPAGED_AREA*. A atualização defeituosa fez com que os sistemas Windows entrassem em um ciclo de reinicialização contínuo, tornando muitos dispositivos inutilizáveis.

2.1. Impacto

- **Global:** A falha impactou usuários em várias regiões do mundo, resultando em perda de acesso a sistemas críticos e serviços essenciais.
- **Serviços Essenciais:** Hospitais, bancos, serviços de emergência, companhias aéreas e sistemas de transporte foram significativamente afetados, aumentando o risco de interrupções nos serviços vitais.
- **Empresas e Usuários:** Muitas empresas e usuários finais enfrentaram paralisações significativas em suas operações diárias, causando transtornos e potencialmente grandes perdas financeiras.

Ações Corretivas e Workaround: A CrowdStrike está trabalhando ativamente para resolver o problema e fornecer atualizações de mitigação. As seguintes ações foram implementadas:

1. **Reversão da Atualização:** A atualização problemática foi revertida para evitar novas ocorrências da BSOD.
2. **Correção do Driver:** Equipes de desenvolvimento estão trabalhando em uma correção para o driver csagent.sys .
3. **Instruções Temporárias:** Foram fornecidas instruções para que os administradores de sistemas afetados possam desativar temporariamente o serviço da CrowdStrike até que uma solução definitiva seja implementada.

2.2. Identificando máquinas afetadas

Query para consulta de máquinas afetadas:

```
// Run with a time frame of "Last 1 day"
#event_simpleName=ConfigStateUpdate event_platform=Win ComputerName=?ComputerName
// Extract the version for channel file 291:
| regex("\|1,123,(?<CFVersion>.*?)\|", field=ConfigStateData, strict=false)
| parseInt(CFVersion, radix=16)
// Group by AID and add the maximum observed channel file version (for the CID) to all results
| groupBy([cid, aid], limit=max, function=selectLast([ComputerName, CFVersion]))
| join(
   query={
      #event_simpleName=ConfigStateUpdate event_platform=Win
ComputerName=?ComputerName
      // Extract the version for channel file 291:
      | regex("\|1,123,(?<CFVersion>.*?)\|", field=ConfigStateData, strict=false)
      | parseInt(CFVersion, radix=16)
      | groupBy(cid, function=max(CFVersion, as=MaxCFVersion))
   }
   , field=cid, include=MaxCFVersion
)
// Filter to only show hosts that have crashed (for any reason)
| join(
   query={
      #event_simpleName=CrashNotification event_platform=Win
ComputerName=?ComputerName
   }
   , field=[cid, aid]
)
// If the host has the N-1 (max minus 1) CF 291 version, assume it is the bad version, if it has any
other version, assume the host is in the clear
| case {
   test(CFVersion == (MaxCFVersion - 1)) | Status:="Update Needed" ;
   //*                              | Status:="OK" ;
}
// Add additional fields for context
| match("aid_master_main.csv", field=aid, include=[Time, AgentVersion, Version, MachineDomain,
OU, SiteName, MAC, LocalAddressIP4])
| formatTime(format="%F %T %Z", as="LastSeen",field=Time)
```

2.3. Workaround

Segue Workaround para reverter o problema:

1. Use o Modo de Segurança e delete o arquivo afetado Você precisará inicializar no Modo de Segurança para seguir o processo. Se você estiver na tela de Recuperação, clique em “Ver opções avançadas de reparo” na tela de Recuperação. No menu Opções Avançadas de Reparo, selecione “Solucionar problemas”, depois escolha “Opções avançadas”. Selecione “Configurações de inicialização” e clique em “Reiniciar”. Depois que seu PC reiniciar, pressione 4 ou F4 para iniciar seu PC no Modo de Segurança. Alternativamente, você também pode desligar o PC, ligá-lo e pressionar repetidamente F8 até o menu Opções Avançadas de Inicialização.

2. A partir daí, selecione Modo de segurança. No Modo de Segurança, abra o Prompt de Comando (admin) ou Windows PowerShell (Admin).

3. No Prompt de Comando, digite o seguinte comando para navegar até o diretório CrowdStrike: cd C:\Windows\System32\drivers\CrowdStrike .

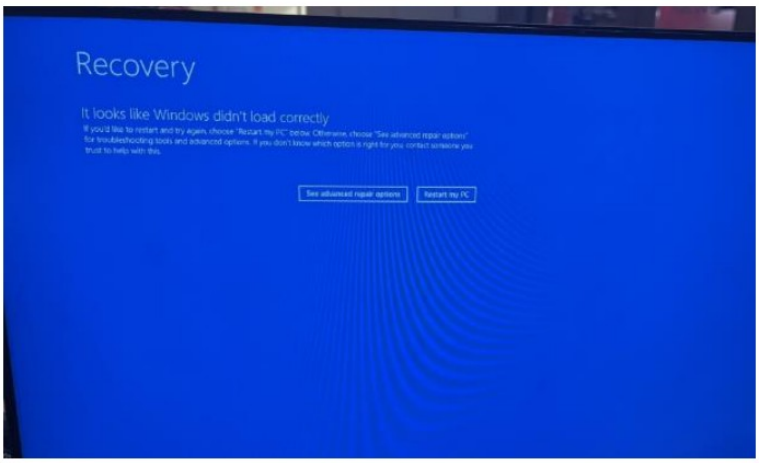
4. Para deletar o arquivo afetado, você precisa localizar o arquivo que corresponde ao padrão C-00000291*.sys.

5. Primeiro, execute o seguinte comando para encontrar o arquivo que corresponde ao padrão: dir C-00000291*.sys.

6. Por exemplo, ele pode ser chamado de algo como C-00000291abc.sys.

7. Depois de identificar o arquivo, delete-o usando del C-00000291.sys

Pode acontecer de mesmo seguindo o Workaround e estarem preso na tela de “Recovery”, caso isso aconteça siga os passos abaixo:



1. Clique em Ver opções avançadas de reparo na tela de Recuperação.

2. No menu Opções Avançadas de Reparo, selecione Solucionar problemas.

3. Em seguida, escolha Opções avançadas.

4. Selecione Configurações de inicialização.

5. Clique em Reiniciar.

6. Depois que seu PC reiniciar, você verá uma lista de opções. Pressione 4 ou F4 para iniciar seu PC no Modo de Segurança.

7. Abra o Prompt de Comando no Modo de Segurança.

8. No Prompt de Comando, navegue até o diretório de drivers: cd \windows\system32\drivers

9. Para renomear a pasta CrowdStrike, use ren CrowdStrike CrowdStrike_old

2.4. Workaround em Clouds Públicas

1. Desconecte o volume de disco do sistema operacional do servidor virtual afetado.

2. Crie um instantâneo ou backup do volume do disco antes de prosseguir como precaução contra alterações não intencionais.

3. Anexe/monte o volume em um novo servidor virtual.

4. Navegue até o diretório C:\Windows\System32\drivers\CrowdStrike.

5. Localize o arquivo correspondente a “C-00000291*.sys” e exclua-o.

6. Desconecte o volume do novo servidor virtual.

7. Reconecte o volume fixo ao servidor virtual afetado.

3. Conclusão

O incidente global envolvendo a atualização do software da CrowdStrike em julho de 2024 destacou a vulnerabilidade das infraestruturas digitais a falhas em sistemas críticos de segurança. A falha no driver csagent.sys, que resultou na Tela Azul da Morte (BSOD) em milhões de dispositivos, teve um impacto profundo em diversos setores, incluindo serviços essenciais como saúde, finanças e transporte.

A resposta da CrowdStrike, que incluiu a reversão da atualização problemática e a implementação de medidas corretivas, foi rápida e decisiva, visando mitigar os danos e restaurar a funcionalidade dos sistemas afetados. No entanto, este evento sublinha a necessidade de procedimentos de teste mais rigorosos e de estratégias de mitigação de risco mais robustas para atualizações de software.

Este relatório forneceu uma visão abrangente do incidente, detalhando as causas, os impactos e as ações tomadas para resolver a situação. A experiência serve como um lembrete crucial da importância de manter práticas de segurança cibernética atualizadas e resilientes para proteger contra interrupções significativas.

Tech Alert CrowStrike: https://supportportal.crowdstrike.com/s/article/Tech-Alert-Windows-crashes-related-to-Falcon-Sensor-2024-07-19


NTT DATA