# O plano da mitigação para Ransomware quer gritar afetando aplicativos baseados Windows Server UCCE

## Índice



## Introdução

Este documento descreve um plano da mitigação para o ransomware chamado quer gritar (igualmente sabido como WannaCry, WanaCrypt0r e WCry) afetando aplicativos baseados Windows Server do Cisco Unified Contact Center Enterprise (UCCE).

Os produtos Microsoft das influências da vulnerabilidade consequentemente recomenda-se fortemente usar os documentos oficiais fornecidos pelo vendedor ou para contactar Microsoft apoie. Este documento é pretendido endereçar algumas das perguntas do ambiente de Cisco UCCE perpective e simplificar a instalação da correção de programa para o ambiente do Contact Center de Cisco.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Sistema operacional de Windows
- Cisco Unified Contact Center Enterprise (UCCE)

## Problema

Os Windows Server que executam o software de Cisco UCCE podem ser afetados pelo malware de Ransomware “querem gritar” (WannaCry, igualmente conhecido como WanaCrypt0r e WCry).

> Nota: A vulnerabilidade esta presente somente em Microsoft Windows baseou o protocolo da versão 1 do bloqueio de mensagem de servidor (SMB) dos sistemas.

Nota: A vulnerabilidade não afeta aplicativos de Cisco UCCE.

Para assegurar-se de que Windows Server não esteja afetado pela vulnerabilidade execute este comando na ferramenta do CMD de Windows.

```
wmic qfe list | findstr "4012212 4012215 4012213 4012216 4015549 4013389"
http://support.microsoft.com/?kbid=4012215 ALLEVICH-F9L4V Security Update KB4012215 NT
AUTHORITY\SYSTEM 4/30/2017
```

Se a saída contém um dos estes KBs o sistema não é vulnerável. Se a saída está vazia você necessidade de instalar a correção de programa correta da Segurança.

**aviso:** O número do hotfix pode ser diferente para seu sistema, assim que é imperativo ao artigo oficial fornecido por Microsoft para determinar a correção de programa correta.

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Um sumário breve de números KB para a maioria de sistemas amplamente utilizados pode ser encontrado abaixo.

- Windows 7 (todas as edições) - KB4012212, KB4012215
- Windows 10 (todas as edições) - KB4012606, KB4013198, KB4013429
- Windows Server 2008 R2 (todas as edições) - KB4012212, KB4012215
- Windows Server 2012 R2 (todas as edições) - KB4012213, KB4012216

# Solução

A correção de programa para a vulnerabilidade foi liberada por Microsoft em março 14, 2017. Os detalhes na correção de programa podem ser encontrados usar este link.

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

A correção de programa pode ser transferida usando este link.

http://www.catalog.update.microsoft.com/Home.aspx

A instalação da correção de programa exige a repartição de Windows Server.

Os clientes são responsáveis para rever toda a atualização da Segurança liberada por Microsoft para Windows, o IIS, e o servidor SQL, e a avaliação de sua exposição de segurança à vulnerabilidade. Leia este boletim para mais detalhes.

http://www.cisco.com/c/en/us/products/collateral/customer-collaboration/unified-contact-center-enterprise/product_bulletin_c25-455396.html