# Een beheerplan voor Ransomware wil een project maken dat gevolgen heeft voor Windows Server-gebaseerde UCCE-toepassingen

## Inhoud



## Inleiding

Dit document beschrijft een matigingsplan voor ransomware genaamd Wanna Cry (ook bekend als WannaCry, WanaCrypt0r en WCry) die de op Windows Server gebaseerde Unified Contact Center Enterprise (UCCE)-toepassingen beïnvloedt.

De kwetsbaarheid heeft gevolgen voor Microsoft-producten en daarom wordt ten zeerste aanbevolen om officiële documenten te gebruiken die door de verkoper zijn geleverd of contact op te nemen met Microsoft-ondersteuning. Dit document is bedoeld om een aantal vragen vanuit Cisco UCCE-omgeving te beantwoorden en de patchinstallatie voor Cisco Contact Center-omgeving te vereenvoudigen.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Windows besturingssysteem
- Cisco Unified Contact Center Enterprise (UCCE)

## Probleem

Windows-servers die Cisco UCCE-software gebruiken, kunnen worden beïnvloed door Ransomware Malware "Wanna Cry" (WannaCry, ook bekend als WanaCrypt0r en WCry).

> Opmerking: De kwetsbaarheid is slechts aanwezig op Microsoft Windows gebaseerde protocol voor systeemservers Message Block (Small Business) versie 1.

> Opmerking: De kwetsbaarheid heeft geen invloed op Cisco UCCE-toepassingen.

Om ervoor te zorgen dat Windows Server niet wordt beïnvloed door de kwetsbaarheid voer deze opdracht in Windows CMD-gereedschap uit.

```
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
```

Als de output een van deze KB's bevat is het systeem niet kwetsbaar. Als de uitvoer leeg is, moet u het juiste veiligheidspleister installeren.

> **Waarschuwing**: Het hotfixnummer kan verschillen voor uw systeem, dus is het verplicht om het officiële artikel van Microsoft te gebruiken om de juiste pleister te bepalen.

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

Hieronder vindt u een korte samenvatting van de KB-nummers voor de meest gebruikte systemen.

- Windows 7 (alle edities) - KB4012212, KB4012215
- Windows 10 (alle edities) - KB4012606, KB4013198, KB4013429
- Windows Server 2008 R2 (alle versies) - KB4012212, KB401215
- Windows Server 2012 R2 (alle versies) - KB401213, KB401216

# Oplossing

De pleister voor de kwetsbaarheid werd op 14 maart 2017 door Microsoft uitgebracht. De details op de pleister zijn te vinden via deze link.

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

U kunt de pleister downloaden via deze link.

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

Voor de installatie van het patches moet de Windows Server opnieuw worden opgestart.

Klanten zijn verantwoordelijk voor het bekijken van een veiligheidsupdate die door Microsoft voor Windows, IS en SQL Server wordt vrijgegeven en het beoordelen van hun veiligheidsblootstelling aan de kwetsbaarheid. Lees dit artikel voor meer informatie.

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.