Eindämmungsplan für Ransomware Wanna Cry, der Windows Server-basierte UCCE-Anwendungen betrifft

Inhalt

Einführung

In diesem Dokument wird ein Eindämmungsplan für Ransomware namens Wanna Cry (auch bekannt als WannaCry, WanaCrypt0r und WCry) mit Auswirkungen auf Windows Server-basierte Cisco Unified Contact Center Enterprise (UCCE)-Anwendungen beschrieben.

Die Schwachstelle betrifft Microsoft-Produkte. Daher wird dringend empfohlen, die offiziellen Dokumente des Anbieters zu verwenden oder sich an den Microsoft-Support zu wenden. Dieses Dokument behandelt einige der Fragen der Cisco UCCE-Umgebung und vereinfacht die Patch-Installation für die Cisco Contact Center-Umgebung.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

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

Problem

Windows-Server mit Cisco UCCE-Software sind möglicherweise von Ransomware-Malware "Wanna Cry" (WannaCry, auch bekannt als WanaCrypt0r und WCry) betroffen.

> **Hinweis**: Die Schwachstelle besteht nur im Microsoft Windows-basierten System Server Message Block (SMB), Protokoll Version 1.

> **Hinweis**: Die Schwachstelle betrifft Cisco UCCE-Anwendungen nicht.

Um sicherzustellen, dass Windows Server nicht von der Schwachstelle betroffen ist, führen Sie diesen Befehl im Windows CMD-Tool aus.

```
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
```

Wenn die Ausgabe eines dieser KBs enthält, ist das System nicht verwundbar. Wenn die Ausgabe leer ist, müssen Sie den richtigen Sicherheits-Patch installieren.

> **Warnung**: Die Hotfix-Nummer kann für Ihr System unterschiedlich sein, daher ist es obligatorisch, den offiziellen Artikel von Microsoft zu finden, um den richtigen Patch.

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

Nachfolgend finden Sie eine kurze Zusammenfassung der KB-Nummern für die am häufigsten verwendeten Systeme.

- Windows 7 (alle Editionen) - KB4012212, KB4012215
- Windows 10 (alle Editionen) - KB4012606, KB4013198, KB4013429
- Windows Server 2008 R2 (alle Editionen) - KB4012212, KB4012215
- Windows Server 2012 R2 (alle Editionen) - KB4012213, KB4012216

Lösung

Der Patch für die Schwachstelle wurde am 14. März 2017 von Microsoft veröffentlicht. Die Details zum Patch finden Sie unter diesem Link.

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

Der Patch kann über diesen Link heruntergeladen werden.

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

Die Patch-Installation erfordert einen Neustart von Windows Server.

Kunden sind dafür verantwortlich, alle von Microsoft für Windows, IIS und SQL Server veröffentlichten Sicherheitsupdates zu überprüfen und ihre Sicherheitsrisiken gegenüber der Schwachstelle zu bewerten. Weitere Einzelheiten finden Sie in diesem Bulletin.

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.