Le plan de réduction pour Ransomware veulent pleurer affectant des applications UCCE basées par Windows Server

Contenu

Introduction

Ce document décrit un plan de réduction pour le ransomware appelé veulent pleurer (également connu comme WannaCry, WanaCrypt0r et WCry) affectant des applications du Cisco Unified Contact Center Enterprise basées par Windows Server (UCCE).

Les Produits de Microsoft d'affects de vulnérabilité donc il est fortement recommandé pour utiliser les documents officiels fournis par le constructeur ou pour entrer en contact avec le support de Microsoft. Ce document est destiné pour aborder certaines des questions de l'environnement de Cisco UCCE perpective et pour simplifier l'installation de correctif pour l'environnement de centre de contact de Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Système d'exploitation Windows
- Cisco Unified Contact Center Enterprise (UCCE)

Problème

Des Windows Server exécutant le logiciel de Cisco UCCE peuvent être affectés par malware de Ransomware « veulent pleurer » (WannaCry, également connu sous le nom de WanaCrypt0r et WCry).

> Remarque: La vulnérabilité est présente seulement sur Microsoft Windows a basé le protocole de version 1 du server message block de systèmes (PME).

> Remarque: La vulnérabilité n'affecte pas des applications de Cisco UCCE.

Pour s'assurer que des Windows Server ne sont pas affectés par la vulnérabilité exécutez cette commande dans l'outil de Windows CMD.

```
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
```

Si la sortie contient un de ces KBS le système n'est pas vulnérable. Si la sortie est vide vous le besoin d'installer le correctif de sécurité correct.

> **Avertissement** : Le nombre de correctif peut être différent pour votre système, ainsi il est obligatoire à l'article officiel fourni par Microsoft pour déterminer le correctif correct.

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

Un résumé rapide des nombres de KO pour la plupart des systèmes très utilisés peut être trouvé ci-dessous.

- Windows 7 (toutes les éditions) - KB4012212, KB4012215
- Windows 10 (toutes les éditions) - KB4012606, KB4013198, KB4013429
- Windows Server 2008 R2 (toutes les éditions) - KB4012212, KB4012215
- Windows Server 2012 R2 (toutes les éditions) - KB4012213, KB4012216

Solution

Le correctif pour la vulnérabilité a été libéré par Microsoft en mars 14, 2017. Les détails sur le correctif peuvent être trouvés utilisant ce lien.

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

Le correctif peut être téléchargé utilisant ce lien.

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

L'installation de correctif exige la réinitialisation de Windows Server.

Les clients sont responsables de passer en revue n'importe quelle mise à jour de sécurité libérée par Microsoft pour Windows, IIS, et Serveur SQL, et évaluer leur risque contre la sécurité à la vulnérabilité. Lisez ce bulletin pour plus de détails.

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