El plan de la mitigación para Ransomware quiere llorar afectando a las aplicaciones basadas Servidor Windows UCCE

Contenido

Introducción

Este documento describe un plan de la mitigación para el ransomware llamado quiere llorar (también conocido como WannaCry, WanaCrypt0r y WCry) afectando a las aplicaciones basadas Servidor Windows del Cisco Unified Contact Center Enterprise (UCCE).

Los productos Microsoft de las influencias de la vulnerabilidad por lo tanto se recomienda fuertemente para utilizar los documentos oficiales proporcionados por el soporte de Microsoft del vendedor o del contacto. Este documento se piensa para dirigir algunas de las preguntas del entorno de Cisco UCCE perpective y para simplificar la instalación de la corrección para el entorno del Centro de contacto de Cisco.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Sistema operativo Windows
- Cisco Unified Contact Center Enterprise (UCCE)

Problema

Los Servidores Windows que funcionan con el software de Cisco UCCE pueden ser afectados por Ransomware que Malware “quiere llorar” (WannaCry, también conocido como WanaCrypt0r y WCry).

> Nota: La vulnerabilidad está presente solamente en Microsoft Windows basó el protocolo de la versión 1 del Bloque de mensaje del servidor (SMB) de los sistemas.

> Nota: La vulnerabilidad no afecta a las aplicaciones de Cisco UCCE.

Para asegurarse de que la vulnerabilidad no afecte al Servidor Windows funcione con este comando en la herramienta del 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
```

Si la salida contiene uno de estos KBs el sistema no es vulnerable. Si la salida está vacía usted necesidad de instalar la corrección correcta de la Seguridad.

> Advertencia: El número del hotfix puede ser diferente para su sistema, así que es obligatorio al artículo oficial proporcionado por el Microsoft para determinar la corrección correcta.

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

Un Resumen breve de números KB para la mayoría de los sistemas ampliamente utilizados se puede encontrar abajo.

- Windows 7 (todas las ediciones) - KB4012212, KB4012215
- Windows 10 (todas las ediciones) - KB4012606, KB4013198, KB4013429
- R2 2008 del Servidor Windows (todas las ediciones) - KB4012212, KB4012215
- R2 del Servidor Windows 2012 (todas las ediciones) - KB4012213, KB4012216

Solución

La corrección para la vulnerabilidad fue liberada por Microsoft en marzo 14, 2017. Los detalles en la corrección se pueden encontrar usando este link.

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

La corrección se puede descargar usando este link.

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

La instalación de la corrección requiere la reinicialización del Servidor Windows.

Los clientes son responsables de revisar cualquier actualización de seguridad liberada por Microsoft para Windows, el IIS, y el SQL Server, y evaluar su riesgo de seguridad a la vulnerabilidad. Lea este boletín para más detalles.

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