Piano di mitigazione per ransomware Wanna Cry che influisce sulle applicazioni UCCE basate su Windows Server

Sommario

Introduzione

Questo documento descrive un piano di mitigazione per i ransomware chiamati Wanna Cry (noti anche come WannaCry, WanaCrypt0r e WCry) che interessano le applicazioni Cisco Unified Contact Center Enterprise (UCCE) basate su Windows Server.

Poiché la vulnerabilità influisce sui prodotti Microsoft, si consiglia di utilizzare i documenti ufficiali forniti dal fornitore o contattare il supporto tecnico Microsoft. Questo documento ha lo scopo di rispondere ad alcune domande dal punto di vista dell'ambiente Cisco UCCE e di semplificare l'installazione delle patch per l'ambiente Cisco Contact Center.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Problema

I server Windows che eseguono il software Cisco UCCE potrebbero essere interessati dal malware ransomware "Wanna Cry" (WannaCry, noto anche come WanaCrypt0r e WCry).

> Nota: la vulnerabilità è presente solo nel protocollo SMB (Server Message Block) versione 1 dei sistemi basati su Microsoft Windows.

Nota: la vulnerabilità non influisce sulle applicazioni Cisco UCCE.

Per assicurarsi che Windows Server non sia influenzato dalla vulnerabilità, eseguire questo comando nello strumento CMD di Windows.

<#root>

```
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 l'output contiene uno di questi KB, il sistema non è vulnerabile. Se l'output è vuoto, è necessario installare la patch di sicurezza corretta.

Avviso: il numero di aggiornamento rapido potrebbe essere diverso per il sistema in uso, pertanto è obbligatorio utilizzare l'articolo ufficiale fornito da Microsoft per determinare la patch corretta.

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

Di seguito è riportato un breve riepilogo dei numeri KB per i sistemi più utilizzati.

- Windows 7 (tutte le edizioni) - KB4012212, KB4012215
- Windows 10 (tutte le edizioni) - KB4012606, KB4013198, KB4013429
- Windows Server 2008 R2 (tutte le edizioni) - KB4012212, KB4012215
- Windows Server 2012 R2 (tutte le edizioni) - KB4012213, KB4012216

Soluzione

La patch per la vulnerabilità è stata rilasciata da Microsoft il 14 marzo 2017. I dettagli sulla patch sono disponibili tramite questo collegamento.

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

La patch può essere scaricata utilizzando questo collegamento.

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

L'installazione della patch richiede il riavvio di Windows Server.

I clienti sono responsabili dell'analisi di qualsiasi aggiornamento della protezione rilasciato da Microsoft per Windows, IIS e SQL Server e della valutazione della loro esposizione alla

vulnerabilità. Leggete questo bollettino per ulteriori informazioni.

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).