План смягчения относительно программного обеспечения с вирусом-вымогателем хочет кричать, влияя на Windows Server базирующиеся приложения UCCE

Содержание

Введение

Этот документ описывает план смягчения относительно r ansomware под названием Хотят Крик (также известный как WannaCry, WanaCrypt0r и WCry), влияние на Windows Server базировало Cisco Unified Contact Center Enterprise (UCCE) приложения.

Уязвимость влияет на продукты Microsoft поэтому, строго рекомендуется использовать официальные документы, предоставленные поставщиком или связаться с поддержкой Microsoft. Этот документ предназначен, чтобы обратиться к некоторым вопросам от Cisco среда UCCE perpective и упростить инсталляцию исправлений для среды Contact Center Cisco.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Операционная система Windows
- Cisco Unified Contact Center Enterprise (UCCE)

Проблема

На Windows Server, выполняющих программное обеспечение Cisco UCCE, может влиять Вредоносное ПО Программного обеспечения с вирусом-вымогателем, "Хотят Крик" (WannaCry, также известный как WanaCrypt0r и WCry).

> **Примечание:** Уязвимость присутствует только на основанном системном протоколе версии 1 Блока сообщений сервера (SMB) Microsoft Windows.

Примечание: Уязвимость не влияет на Cisco приложения UCCE.

Чтобы гарантировать, что на Windows Server не влияет уязвимость, выполняет эту команду в программном средстве 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
```

Если выходные данные содержат один из этих КБИТ, система не уязвима. Если выходные данные пусты, необходимо установить корректный патч безопасности.

% Warning: Номер исправления может быть другим для вашей системы, таким образом, это является обязательным к официальной статье, предоставленной Microsoft для определения корректного исправления.

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

Краткое резюме номеров КБ для наиболее широко используемых систем может быть найдено ниже.

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

Решение

Исправление для уязвимости было освобождено Microsoft 14 марта 2017. Подробные данные об исправлении могут быть найдены с помощью этой ссылки.

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

Исправление может быть загружено с помощью этой ссылки.

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

Инсталляция исправлений требует перезагрузки Windows Server.

Клиенты ответственны за рассмотрение любого обновления системы защиты, освобожденного Microsoft для Windows, IIS, и Сервера SQL и оценки их угрозы безопасности к уязвимости. Считайте этот бюллетень для получения дополнительной информации.

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