Mitigation Plan for Ransomware Wanna Cry Affecting Windows Server Based UCCE Applications

Contents

Introduction

This document describes a mitigation plan for ransomware called Wanna Cry (also known as WannaCry, WanaCrypt0r and WCry) affecting Windows Server based Cisco Unified Contact Center Enterprise (UCCE) applications.

The vulnerability affects Microsoft products therefore it is strongly recommended to use official documents provided by the vendor or contact Microsoft support. This document is intended to address some of the questions from Cisco UCCE environment perpective and simplify the patch installation for Cisco Contact Center environment.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Windows Operating System
- Cisco Unified Contact Center Enterprise (UCCE)

Problem

Windows Servers running Cisco UCCE software may be affected by Ransomware Malware "Wanna Cry" (WannaCry, also known as WanaCrypt0r and WCry).

> **Note**: The vulnerability is present only on Microsoft Windows based systems Server Message Block (SMB) version 1 protocol.

> **Note**: The vulnerability does not affect Cisco UCCE applications.

To ensure that Windows Server is not affected by the vulnerability run this command in Windows CMD tool.

```
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
```

If the output contains one of these KBs the system is not vulnerable. If the output is empty you need to install correct security patch.

> **Warning**: Hotfix number may be different for your system, so it is mandatory to the official article provided by Microsoft to determine the correct patch.

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

A brief summary of KB numbers for most widely used systems may be found below.

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

Solution

The patch for the vulnerability was released by Microsoft on March 14, 2017. The details on the patch can be found using this link.

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

The patch can be downloaded using this link.

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

The patch installation requires Windows Server reboot.

Customers are responsible for reviewing any security update released by Microsoft for Windows, IIS, and SQL Server, and assessing their security exposure to the vulnerability. Read this bulletin for more details.

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