Patching the SP6300 Against Wannacry Ransomware

User Guide

KEYSIGHT
TECHNOLOGIES

Notices

Copyright Notice

Revision

Revision 0.1, 30th May 2017

Published by:

Keysight Technologies, Inc.
Harvest Crescent
Fleet, Hampshire
UK, GU51 2UZ

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

Declaration of Conformity

Declarations of Conformity for this product and for other Keysight products may be downloaded from the Web. Go to http://www.keysight.com/go/conformity and click on "Declarations of Conformity." You can then search by product number to find the latest Declaration of Conformity.

U.S. Government Rights

The Software is "commercial computer software," as defined by Federal Acquisition Regulation ("FAR") 2.101. Pursuant to FAR 12.212 and 27.405-3 and Department of Defense FAR Supplement ("DFARS") 227.7202, the U.S. government acquires commercial computer software under the same terms by which the software is customarily provided to the public. Accordingly, Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at http://www.keysight.com/find/sweula. The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or (2) Relinquish to, or otherwise provide, the government rights in excess of these rights customarily provided to the public to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation. No additional government requirements beyond those set forth in the EULA shall apply, except to the extent that those terms, rights, or licenses are explicitly required from all providers of commercial computer software pursuant to the FAR and the DFARS and are set forth specifically in writing elsewhere in the EULA. Keysight shall be under no obligation to update, revise or otherwise modify the Software. With respect to any technical data as defined by FAR 2.101, pursuant to FAR 12.211 and 27.404.2 and DFARS 227.7102, the U.S. government acquires no greater than Limited Rights as defined in FAR 27.401 or DFAR 227.7103-5 (c), as applicable in any technical data.

Warranty

THE MATERIAL CONTAINED IN THIS DOCUMENT IS PROVIDED "AS IS," AND IS SUBJECT TO BEING CHANGED, WITHOUT NOTICE, IN FUTURE EDITIONS. FURTHER, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, KEYSIGHT DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED WITH REGARD TO THIS MANUAL AND ANY INFORMATION CONTAINED HEREIN, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. KEYSIGHT SHALL NOT BE LIABLE FOR ERRORS OR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, USE, OR PERFORMANCE OF THIS DOCUMENT OR ANY INFORMATION CONTAINED HEREIN. SHOULD KEYSIGHT AND THE USER HAVE A SEPARATE WRITTEN AGREEMENT WITH WARRANTY TERMS COVERING THE MATERIAL IN THIS DOCUMENT THAT CONFLICT WITH THESE TERMS, THE WARRANTY TERMS IN THE SEPARATE AGREEMENT WILL CONTROL.

Customer support

It is our goal to provide you with excellent Customer Support. To request assistance with any aspect of your Anite test system, please create a Help Desk Request (HDR) using the Anite Help Desk. For other queries, please email customersupport.di@keysight.com.

To access the Anite Help Desk, and to download the latest releases of software and documentation, please log in to myKeysight. On the myKeysight home page, in the Quick Links box, click the link for the Anite Help Desk, or click Keysight Software Manager for software downloads.

.

CONTENTS

1 INTRODUCTION

This document describes the procedure for patching the StarPoint SP6300 TD-SCDMA Protocol Analyze Tester (hereafter referred to as SP6300) against the WannaCry ransomware attack. It also describes the correct configuration of the test system to protect against future attacks.

1.1 Scope

This document is intended to be read by both Customer Services, and by customers who have SP6300 units in their test system.

The patching process described in this document should only be undertaken by engineers with experience of administrating Windows PCs.

2 PATCHING A STARPOINT SP6300

2.1 Overview

The SP6300 contains an embedded PC which runs the 32-bit version of Windows XP. This version of the operating system contains a vulnerability in the Server Message Block (SMB) protocol which is exploited by the WannaCry ransomware.

Microsoft have released a patch for the vulnerability and Keysight recommend that all SP6300 systems be taken offline and patched immediately. For readers who are interested in the background, Microsoft have provided Customer Guidance for WannaCrypt Attacks here.

2.2 Procedure for Patching the StarPoint SP6300

2.2.1 Prepare the SP6300

1. Stop any test runs which are currently in progress.
2. Power down and disconnect the SP6300 from the test system.
3. Ensure the SP6300 is disconnected from any/all networks for the duration of the patching activity.
4. Connect a keyboard & mouse to the SP6300's USB ports, and a suitable monitor to the SP6300 VGA port.

2.2.2 Disable "autorun.inf"

To prevent accidental or malicious infection of the SP6300 through a USB Memory Stick, Keysight strongly recommends that autorun should be disabled. The process for disabling autorun requires changes to the registry. Errors made whilst editing the registry can have catastrophic consequences: backing up the registry is strongly recommended before changing it in any way.

Perform the following steps to back up the registry:

1. Click Start, click Run, type "regedit" in the Open box & click OK.
2. When the Registry Editor window opens, select File / Export.
3. In the "File name" field enter a name for the backup file.
4. In the "Save as type" field, select "Registration Files (*.reg)"
5. In the "Export Range" area, select the "All" option
6. Click Save.

Perform the following steps to disable autorun:

1. If the Registry Editor is not already open, click Start, click Run, type "regedit" in the Open box & click OK.
2. Locate and click the following key in the registry:

   HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\NoDriveTypeAutorun
3. Right-click NoDriveTypeAutoRun and select "Modify".
4. In the value data box, enter 0xFF. If the value shown is already 0xFF then no action is required for this step.
5. Click OK, then exit the Registry Editor.

These steps are also described in a Microsoft Support article here.

2.2.3 Install Patch KB 4012598

1. Using a PC which is connected to the internet, download the "Windows XP SP3 x86" version of the patch from the Microsoft website (here). Do not use the SP6300 to download the patch.
2. Copy the patch to a USB2 Memory Stick (Windows XP does not support USB3). Virus check the memory stick to ensure it has not inadvertently become infected.

3. Insert the memory stick to the USB hub connected to the SP6300 and open it using Windows File Explorer.

4. Run the KB4012598 patch, for example:

   windowsxp-kb4012598-x86-custom-enu_*.exe

5. Shutdown the SP6300.

2.2.4 Reconnect the SP6300 to the test system

1. Reconnect the SP6300 to the test system.

2. Check the configuration of the test system to ensure it is correctly isolated from external networks. This is achieved by ensuring any external network are only connecting to the Test System PC. The default configuration of the Test System PC is to isolate the Test System network from other networks and this configuration must not be changed (for example, by updating the routing tables),

   See Figure 1, which shows the correct way of connecting a test system to a corporate network.

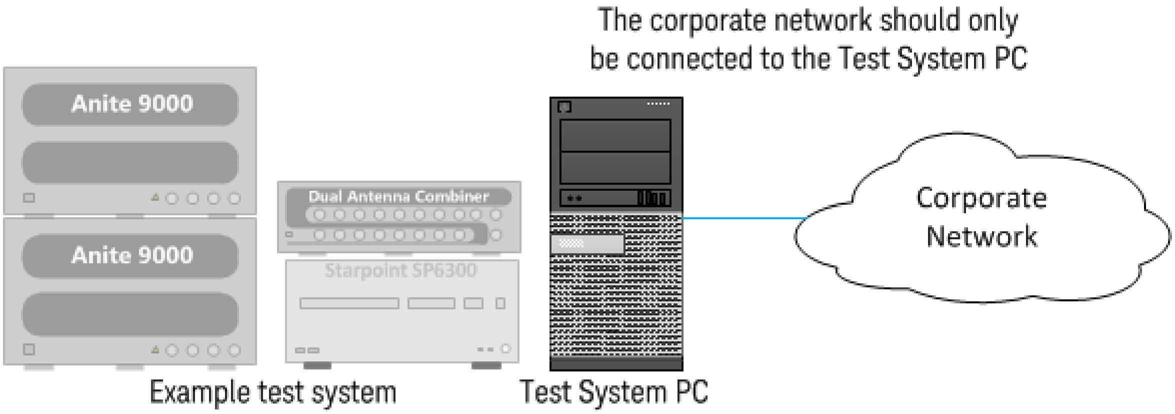

Figure 1: Connecting external networks to a test system

3. Confirm that the test system is behaving correctly by running a small number of TD-LTE<>TD-SCDMA inter-RAT test cases against a device which is known to pass those test cases.