Security Advisory - Buffer Overflow in Huawei UTPS Back-End

SA. No. Huawei-SA-20120922-01-UTPS **Release Date** 22nd Sep. 2012

Summary

The back-end software UTPS is the application software which is operated on the management data card of PC to realize the configuration and dial-up connection of data card, instant messages receiving and sending, telephone directory management and the like. The current product has a vulnerability：

The UTPS1.0 back-end does not fully verify the incoming parameters when copying the character strings during the process of uploading the plug-in configuration files, which leads to the overflow（HWNSIRT-2012-0994). As a result, the script which is specified by some malicious users may be executed to run the application program which is specified by the malicious users.

This vulnerability is reported by Dark-Puzzle from Inj3ct0r TEAM.

Currently, workarounds are available and are listed below. Huawei has also made the version plan to resolve this vulnerability.

Affected versions:

Product Name	Back-End Version Number
E173u-1	UTPS11.302.09.06.162
E153u-1	UTPS11.302.09.05.162
E1550	UTPS11.302.09.01.162
E1550	UTPS11.302.09.05.162
E1550	UTPS11.302.09.01.162
E1750	UTPS11.302.09.03.162
E1690	UTPS11.302.09.02.162
E220	UTPS11.002.03.09.162
E220	UTPS11.002.03.03.162
E630	UTPS11.002.03.04.162
E5830	UTPS16.002.10.04.04
E1550	UTPS16.002.10.02.04
E180	UTPS11.300.05.01.04
E180	UTPS11.300.05.02.04
E169	UTPS11.002.04.03.04
E156G	UTPS11.300.05.02.04
EC122	UTPS16.001.05.06.649

Impact

The security vulnerability may be utilized by malicious users to run the specified programs.

Vulnerability Scoring Details

The vulnerability classification has been performed by using the CVSSv2 scoring system (http://www.first.org/cvss/).

Base Score: 6.9 (AV: L/AC: M/Au:N/C:C/I:C/A:C)

Temporal Score: 6.2 (E: F/RL: W/RC: C)

Technique Details

The back-end does not fully verify the incoming parameters when copying the character strings during the process of uploading the plug-in configuration files, and the character strings have not been checked before copying. If there is a long character string saved in the configuration files, the copying execution will lead to the overflow of the invoked buffer:

1. Prerequisite:

Obtain the local user privilege；

2. Attacking procedure:

Modify the configuration file, and save a long character string in the specified attribute. Execute the program which will lead to the overflow of the invoked buffer;

;

3. Impact:

The security vulnerability may be utilized by malicious users to run the specified programs.

Temporary Fix

Users of Windows can upgrade the operation system to Windows XP sp3 directly or can download UTPS2.0 from our web site to cope with the security vulnerability.

1. Users of Windows XP sp1 can log in to the Web site of Microsoft to install the patch Windows XP sp3.

2. Users of the operation systems of higher versions will not be affected.

Software Versions and Fixes

The below affected products can deploy the workarounds mentioned above to mitigate the risks, or be upgraded to the below versions：

Product Model	Back-End Version	Solved Version	Solved Time
E173u-1	UTPS11.302.09.06.162	UTPS21.005.22.00.162_MAC21.005.22.01.162	2012-9-26
E153u-1	UTPS11.302.09.05.162	UTPS21.005.15.06.162_MAC21.005.15.01.162	2012-9-26

The other affected products can deploy the workarounds mentioned above to mitigate the risks, and there is no new version or patch to be released.

FAQs

1. How to identify the version I am using is Version 1.0 or Version 2.0?

Answer: Select the menu of *Help-->About XXX*, in which XXX refers to the name of the software. In the displayed page, you can view the version number of the software to be Software Name 16.002.37.00.03. Any version whose number is started with 1 may have the security vulnerability.

2. I bought the data care recently, and its version is different from the mentioned one. I wonder if it may have the same vulnerability.

Answer: Check the version according to the mentioned methods and you can figure it out there is vulnerability if it is Version 1.0.

Obtaining Fixed Software

http://www.huaweidevice.com/

Contact Channel for Technique Issue

PSIRT@huawei.com

Revision History

22nd Sep, 2012 V1.0 INITIAL

Exploitation and Vulnerability Source

This vulnerability is reported by Dark-Puzzle from Inj3ct0r TEAM (http://packetstormsecurity.org/files/download/116604/huawei-overflow.txt). The Huawei PSIRT is not aware of any malicious use launched to attack through the vulnerability described in this advisory.

Declaration

This document is provided on an "AS IS" basis and does not imply any kind of guarantee or warranty, either express or implied, including the warranties of merchantability or fitness for a particular purpose. In no event shall Huawei Investment & Holding Co., Ltd. or any of its directly or indirectly controlled subsidiaries or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages. Your use of the document, by whatsoever means, will be totally at your own risk. Huawei is entitled to amend or update this document from time to time.

The information and data embodied in this document and any attachment are strictly confidential information of Huawei and are supplied on the understanding that they will be held confidentially and not disclosed to third parties without the prior written consent of Huawei. You shall use all reasonable efforts to protect the confidentiality of information. In particular, you shall not directly or indirectly disclose, allow access to, transmit or transfer the information to a third party without our prior written consent. Thank for your co-operation.

Huawei Security Procedures

Contact us through PSIRT@huawei.com if you need to:

1. Provide feedback on security vulnerability of Huawei products.

2. Get support for Huawei security incident response services.

3. Obtain Huawei security vulnerability information.