

UNITROL 1000 Application Notes 1310_0255

CMT 1000 Vulnerability bug fix

Summary

A third party component, which is used in CMT UN1000 software for Windows PCs, is vulnerable to ActiveX execution.

An attacker who successfully exploits this vulnerability could run arbitrary code on a computer where the product is installed.

The security of the affected PC can be reestablished by installing the latest CMT 1000 Release 6.101.

ABB recommends to install the latest CMT1000 Release 6.101 to secure your PC against hacker attacks.

Hardware Version	<input checked="" type="checkbox"/> UNITROL 1000-15 Status Serial no	<input checked="" type="checkbox"/> UNITROL 1000-7 Status Serial no
	<input checked="" type="checkbox"/> UNITROL 1020 Status Serial no	<input checked="" type="checkbox"/> UNITROL 1010 Status Serial no
	<input checked="" type="checkbox"/> UNITROL 1000-PM40 Status Serial no	
Software Version	Panel SW	NA
	Target SW	NA
	CMT 1000	4.xxx / 5.xxx / 6.xxx


Based on		Project		UNITROL 1000	
Prepared by	Rudolf Moeckli	29.10.13	AN 1310_0255		
Approved by	Rene Pulfer	29.10.13	Responsible Department	ATPE	
Title UNITROL 1000 Application Notes, Title					
 ABB Switzerland Ltd	Document number		Language	Rev. ind.	Page
	3BHS538288 E08		en	-	1 Number of pages 6

Table of Contents

TABLE OF CONTENTS	2
CHAPTER 1 - PROBLEM DESCRIPTION	3
1.1. Problem overview.....	3
1.2. Affected applications	3
1.3. Vulnerability details	3
CHAPTER 2 - SOLUTIONS	4
2.1. How to solve	4
2.1.1. <i>Installation of different Releases</i>	4
2.1.2. <i>Compatibility</i>	4
2.2. Download latest CMT	4
CHAPTER 3 - URGENCY OF ACTION(S)	6
REVISION	6

Chapter 1 - Problem Description

1.1. Problem overview

A third party component, which is used in the CMT UN1000 software for Windows PCs, is vulnerable to ActiveX execution.

An attacker who successfully exploits this vulnerability could run arbitrary code on a computer where the product is installed.

1.2. Affected applications

Affected are all PC's where the CMT1000 SW is installed. Practically all following releases are affected:


- Release 4.xxx (UNITROL 1000-15 / UNITROL 1000-7)
- Release 5. xxx (UNITROL 1000-15 / UNITROL 1000-7)
- Release 6.xxx (UNITROL 1010 / UNITROL 1020)

The vulnerability is only affecting PC's, where CMT 1000 SW is installed. UNITROL 1000 applications in operations are not affected.

1.3. Vulnerability details

The vulnerability originates from a third party ActiveX component that can allow component execution on the affected PC.

An attacker can build a website that exploits this ActiveX control to download files to any location accessible by the user.

	ABB Switzerland Ltd	Document Nr. 3BHS538288 E08	Language en	Rev. Ind. -	page 3
---	----------------------------	---------------------------------------	----------------	----------------	-----------

Chapter 2 - Solutions

2.1. *How to solve*

Vulnerability can be solved by installing the latest CMT 1000 Release 6.101. The tool includes a batch to reestablish security of the PC.

2.1.1. *Installation of different Releases*

Installation of several different CMT 1000 releases are possible. In case you have older CMT1000 release (4.xxx / 5.xxx / 6.0xx) installed, you have to install only the latest CMT 1000 Release 6.101. The older versions are still full functional.

2.1.2. *Compatibility*

Latest CMT 1000 Release 6.101 is only working with Target Release 6.xxx. Target main release number (e.g. 5.xxx) must fit to main release of CMT 1000 (e.g. 5.xxx).


Therefore older CMT 1000 SW releases should not be deinstalled.

2.2. *Download latest CMT*

ABB provides accessibility to the database via internet for customers to access brochures, manuals, and SW. The database access is managed by user name and password. The password is valid for 1 month after distributing this application note.

In case the time is escalated and access with the given password is blocked, contact UNITROL 1000 support line:

unitrol1000support@ch.abb.com

	ABB Switzerland Ltd	Document Nr. 3BHS538288 E08	Language en	Rev. Ind. -	page 4
---	---------------------	---------------------------------------	----------------	----------------	-----------

Access information to download CMT1000

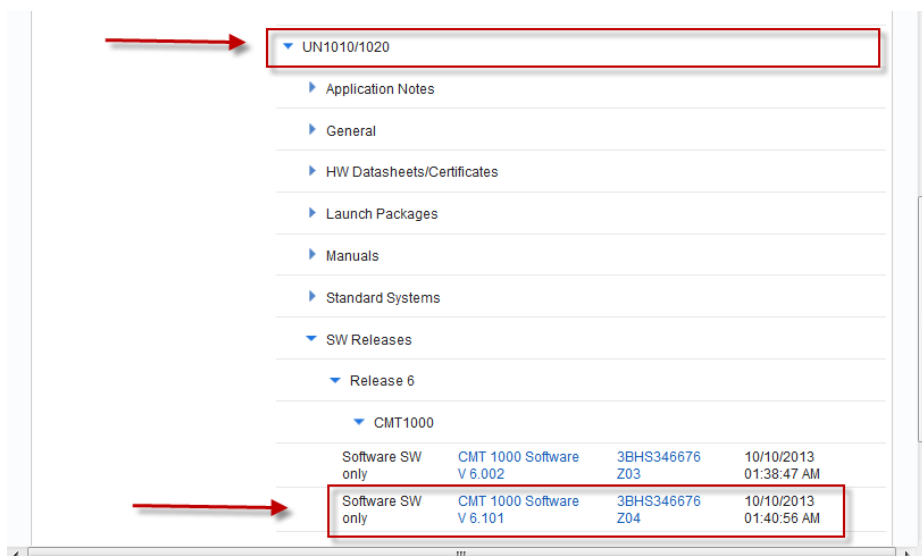
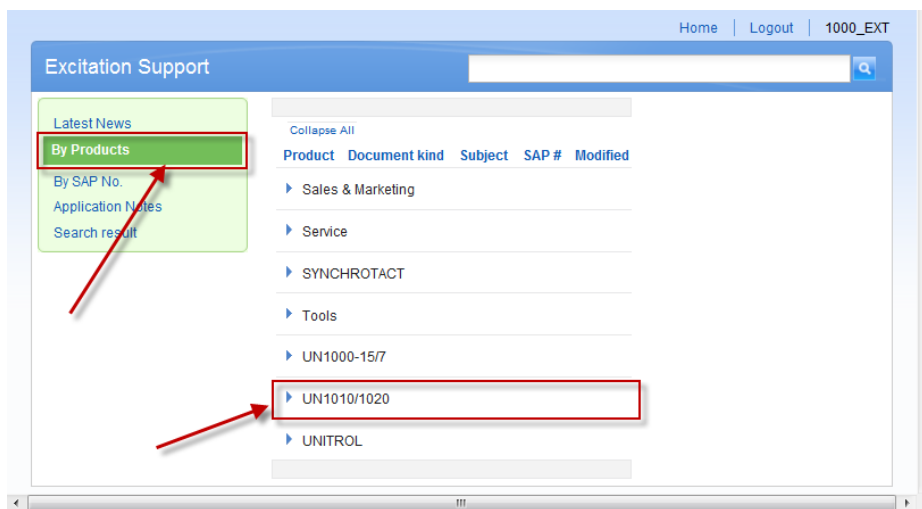
Web link: <http://domino.de.abb.com/db/db0007/db002796.nsf/Home.xsp>

User name: **1000_EXT**

Password: **GE9cKIfBlq**

Navigate within database to download the CMT 1000:

- Select Filter “By Product”
- Open Folder “UNITROL 1010/1020”
- Open Folder “SW Releases / Release 6 / CMT1000



Chapter 3 - Urgency of action(s)

<input type="checkbox"/> A) Information only => No special action necessary
<input type="checkbox"/> B) Fix it when occurring
<input checked="" type="checkbox"/> C) Fix it at next occasion (Factory Testing, Commissioning, Site Service)
<input type="checkbox"/> D) Fix it proactively - Inform customer and define date when case can be
<input type="checkbox"/> E) Same as D) but additionally <ul style="list-style-type: none">- Send action plan to PRU- Inform PRU when action(s) are completed

REVISION

Rev. ind.	Page (P) Chapt.(C)	Description	Date Dept./Init.
-	All	Initial Version	29.10.13 R. Moeckli ATPE-PM