SSA-198330: Local Privilege Escalation in TD Keypad Designer

Publication Date: 2018-09-11
Last Update: 2018-09-11
Current Version: V1.0
CVSS v3.0 Base Score: 7.3

SUMMARY

All versions of the TD Keypad Designer for printing customized lamination sheets for Text Display devices are affected by a DLL hijacking vulnerability that could allow a local low-privileged attacker to escalate his privileges.

Text Display devices and TD Keypad Designer have been discontinued in 2012 and were replaced by KTP Basic with option Express Design.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIEMENS TD Keypad Designer: All versions	See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Restrict write permissions to directories with TD project files to authorized users.
- Only open TD projects from trusted sources.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

TD Keypad Designer is a tool for printing customized lamination sheets for Text Display devices.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

Vulnerability CVE-2018-13806

A DLL hijacking vulnerability exists in all versions of SIEMENS TD Keypad Designer which could allow an attacker to execute code with the permission of the user running TD Designer.

The attacker must have write access to the directory containing the TD project file in order to exploit the vulnerability. A legitimate user with higher privileges than the attacker must open the TD project in order for this vulnerability to be exploited.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	7.3
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2018-09-11):	Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.