SSA-163226: CELL File Parsing Vulnerability in Tecnomatix RobotExpert

Publication Date: 2021-04-13
Last Update: 2021-04-13
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

Siemens Tecnomatix RobotExpert version V16.1 fixes a vulnerability that could be triggered when the application reads CELL files. If a user is tricked to open a malicious file with the affected application, this could lead to a crash, and potentially also to arbitrary code execution or data extraction on the target host system.

Siemens recommends to update to the latest version and to avoid opening of untrusted files from unknown sources.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Tecnomatix RobotExpert: All versions < V16.1	Update to V16.1 or later version https://support.sw.siemens.com/ (login required)

WORKAROUNDS AND MITIGATIONS

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

- Do not open untrusted CELL files from unknown 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

RobotExpert is an easy-to-deploy, robot simulation and offline programming software that enables you to perform complete 3D modeling, visualization and simulation of your automation systems including robots, tooling and peripheral equipment.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (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.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2021-25670

Affected applications lack proper validation of user-supplied data when parsing CELL files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12608)

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Trend Micro Zero Day Initiative for coordinated disclosure
- Cybersecurity and Infrastructure Security Agency (CISA) for coordination efforts

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 (2021-04-13): Publication Date

TERMS OF USE