SSA-786743: Code Injection Vulnerability in Advanced Reporting for Desigo CC and Desigo CC Compact

Publication Date: 2020-08-11
Last Update: 2020-08-11
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

The extension module Advanced Reporting for Desigo CC and Desigo CC Compact contains a code injection vulnerability, which could be exploited if the extension module is installed on the server and configured.

Siemens has released patches for the affected products and recommends specific countermeasures for unpatched systems.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Desigo CC: V4.x	Apply the patch provided through Siemens online support: https://support.industry.siemens.com/cs/ww/en/view/109780860 (Login required)
Desigo CC: V3.x	Apply the patch provided through Siemens online support: https://support.industry.siemens.com/cs/ww/en/view/109780956 (Login required)
Desigo CC Compact: V4.x	Apply the patch provided through Siemens online support: https://support.industry.siemens.com/cs/ww/en/view/109780860 (Login required)
Desigo CC Compact: V3.x	Apply the patch provided through Siemens online support: https://support.industry.siemens.com/cs/ww/en/view/109780956 (Login required)

WORKAROUNDS AND MITIGATIONS

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

- If the extension module Advanced Reporting is already installed, apply the patch as documented above
- In all other cases avoid the installation of the extension module from existing deliveries of Desigo CC or Desigo CC Compact software, until you receive an updated version of the software that includes the patch already.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure Siemens strongly recommends to protect network access to affected products with appropriate mechanisms. It is advised to follow recommended security practices in order to

run the devices in a protected IT environment.

PRODUCT DESCRIPTION

Desigo CC is the integrated building management platform for managing high-performing buildings. With its open design, it has been developed to create comfortable, safe and efficient facilities. It is easily scalable from simple single-discipline systems to fully integrated buildings.

Desigo CC Compact extends the portfolio with a tailored solution for small and medium-sized buildings.

Advanced Reporting for Desigo CC and Desigo CC Compact is an optional extension module that allows customers to create sophisticated reports with many widgets (e.g. bar-charts, . . .) to monitor and compare over time selected KPIs.

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-2020-10055

Affected applications are delivered with a 3rd party component (BIRT) that contains a remote code execution vulnerability if the Advanced Reporting Engine is enabled.

The vulnerability could allow a remote unauthenticated attacker to execute arbitrary commands on the server with SYSTEM privileges.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
CWE	CWE-94: Improper Control of Generation of Code ('Code Injection')

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 (2020-08-11): 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.