SSA-453715: Deserialization Vulnerability in CCOM Communication Component of Desigo CC Family

Publication Date: 2021-09-14
Last Update: 2021-09-14
Current Version: V1.0
CVSS v3.1 Base Score: 10.0

SUMMARY

Desigo CC, Desigo CC Compact and Cerberus DMS that use CCOM communication component hosted in IIS contain a deserialisation vulnerability that could allow an unauthenticated attacker to perform remote code execution. Only those systems that use Windows App and/or IE XBAP Web Client are affected. Regular installed clients and the new HTML5 Flex Clients are not impacted by this vulnerability.

Note that the risk of this vulnerability being exploited is particularly high for any Desigo CC system that is connected directly to the Internet. For systems not accessible directly from the Internet, an attacker would need to have access to the local network to exploit this vulnerability.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Cerberus DMS V4.0: All versions	Apply Patch 1520637 https://support.industry.siemens.com/cs/document/109801179/
Cerberus DMS V4.1: All versions	Apply Patch 1417968 https://support.industry.siemens.com/cs/document/109801179/
Cerberus DMS V4.2: All versions	Update to V4.2 QU1 and Apply Patch 1417967 https://support.industry.siemens.com/cs/document/109801179/
Cerberus DMS V5.0: All versions < v5.0 QU1	Update to V5.0 QU1 or later version https://support.industry.siemens.com/cs/document/109800951/
Desigo CC Compact V4.0: All versions	Apply Patch 1520637 https://support.industry.siemens.com/cs/document/109801179/
Desigo CC Compact V4.1: All versions	Apply Patch 1417968 https://support.industry.siemens.com/cs/document/109801179/
Desigo CC Compact V4.2: All versions	Update to V4.2 QU1 and Apply Patch 1417967 https://support.industry.siemens.com/cs/document/109801179/
Desigo CC Compact V5.0: All versions < V5.0 QU1	Update to V5.0 QU1 or later version https://support.industry.siemens.com/cs/document/109800951/
Desigo CC V4.0: All versions	Apply Patch 1520637 https://support.industry.siemens.com/cs/document/109801179/

Desigo CC V4.1: All versions	Apply Patch 1417968 https://support.industry.siemens.com/cs/document/109801179/
Desigo CC V4.2: All versions	Update to V4.2 QU1 and Apply Patch 1417967 https://support.industry.siemens.com/cs/document/109801179/
Desigo CC V5.0: All versions < V5.0 QU1	Update to V5.0 QU1 or later version https://support.industry.siemens.com/cs/document/109800951/

WORKAROUNDS AND MITIGATIONS

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

- If the user is using a software version equal or older than V3.x, no patches will be released. Siemens recommends to upgrade to V5.0 QU1 (or any newer version that will be released in the future).
- If a patch or Quality Update is not feasible, and if the user can accept to stop the use of Windows App and IE XBAP Web Client, then disable the Web Application and Web Client from SMC. As a result, Windows App and IE XBAP Web Client will stop working and the vulnerability cannot be exploited anymore.
- If all the above cannot apply, restrict Desigo CC to dedicated local networks, disabling the Internet access by blocking the CCOM Port for inbound and outbound communication. This will allow the use of Windows App and IE XBAP Client within a defined network space like the local network only. This action requires approval from the user as it will not remove the vulnerability but reduce the exposure. The vulnerability can be exploited in case the attacker can access the protected network first.

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

Cerberus DMS is a danger management station that helps users manage fire safety and security events.

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.

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-2021-37181

The application deserialises untrusted data without sufficient validations, that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system. The CCOM communication component used for Windows App / Click-Once and IE Web / XBAP client connectivity are affected by the vulnerability.

CVSS v3.1 Base Score	10.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-502: Deserialization of Untrusted Data

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Markus Wulftange from Code White GmbH for reporting the vulnerability

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 (2021-09-14):	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.