# SSA-836027: Client-side Authentication in Desigo CC and Cerberus DMS

| | |
|---|---|
| Publication Date: | 2022-10-11 |
| Last Update: | 2022-10-11 |
| Current Version: | V1.0 |
| CVSS v3.1 Base Score: | 9.8 |

## SUMMARY

Desigo CC and Cerberus DMS are based on SIMATIC WinCC OA and implement client-side only authentication for specific parts of their client-server communication. In this configuration, attackers could impersonate other users or exploit the client-server protocol without being authenticated, as documented for SIMATIC WinCC OA in SSA-111512 [1].

Siemens recommends specific mitigations, documented in [2], for products where fixes are not, or not yet available. Additional details regarding these mitigations can be found in the chapter Additional Information.

[1] https://cert-portal.siemens.com/productcert/html/ssa-111512.html
[2] https://support.industry.siemens.com/cs/ww/en/view/109813389/

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| Cerberus DMS:<br>All versions | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| Desigo CC:<br>All versions | Currently no fix is available<br>See recommendations from section Workarounds and Mitigations |
| Desigo CC Compact:<br>All versions | Currently no fix is available<br>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:

- See https://support.industry.siemens.com/cs/ww/en/view/109813389/ for a list of specific mitigations

Please follow the General Security Recommendations.

## 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-2022-33139

Affected applications use client-side only authentication, when neither server-side authentication (SSA) nor Kerberos authentication is enabled.

In this configuration, attackers could impersonate other users or exploit the client-server protocol without being authenticated.

| | |
|---|---|
| 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:P/RL:O/RC:C |
| CWE | CWE-603: Use of Client-Side Authentication |

## 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 (2022-10-11): | 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.