SSA-226339: Multiple Web Application Vulnerabilities in Desigo Insight

Publication Date:	2020-10-13
Last Update:	2020-10-13
Current Version:	V1.0
CVSS v3.1 Base Score:	5.4

SUMMARY

The latest hotfix for Desigo Insight fixes three vulnerabilities that have been identified in the web server, including SQL injection (CVE-2020-15792), clickjacking (CVE-2020-15793), and full path disclosure (CVE-2020-15794).

Siemens recommends updating to the latest version of Desigo Insight and to apply the hotfix.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Desigo Insight: All versions	Update to V6.0 SP5 and apply Hotfix 2 or later https://support.industry.siemens.com/cs/ww/en/view/109781922

WORKAROUNDS AND MITIGATIONS

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

- Disable Desigo Insight Web, if not used. Alternatively, restrict the access to allow only authorized users to access the web application
- CVE-2020-15793: Only access links from trusted sources in the browser you use to access Desigo Insight Web

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 Insight is the BACnet management station of the Desigo building automation and control system that works with the automation stations Desigo PX, Desigo TRA (Total Room Automation) and BACnet third-party.

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-2020-15792

The web service does not properly apply input validation for some query parameters in a reserved area.

This could allow an authenticated attacker to retrieve data via a content-based blind SQL injection attack.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command (‘SQL Injection’)

Vulnerability CVE-2020-15793

The device does not properly set the X-Frame-Options HTTP Header which makes it vulnerable to Clickjacking attacks.

This could allow an unauthenticated attacker to retrieve or modify data in the context of a legitimate user by tricking that user to click on a website controlled by the attacker.

CVSS v3.1 Base Score	5.4
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-1021: Improper Restriction of Rendered UI Layers or Frames

Vulnerability CVE-2020-15794

Some error messages in the web application show the absolute path to the requested resource.

This could allow an authenticated attacker to retrieve additional information about the host system.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Davide De Rubeis, Damiano Proietti, Matteo Brutti, Stefano Scipioni, and Massimiliano Brolli from TIM Security Red Team Research for coordinated disclosure

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 (2020-10-13): 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.