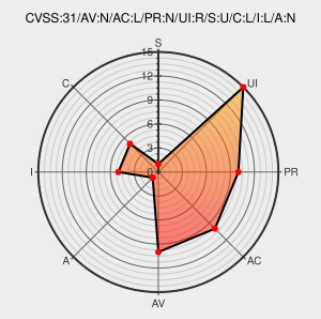
CVE-2020-15793

Published on: 10/15/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:41 PM UTC

CVE-2020-15793

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Desigo Insight from Siemens contain the following vulnerability:

A vulnerability has been identified in Desigo Insight (All versions). 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.

CVE-2020-15793 has been assigned by productcert@siemens.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Siemens** - **Desigo Insight** version **All versions**

CVSS3 Score: 5.4 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	LOW	NONE

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link

Siemens Desigo Insight | CISA	Third Party Advisory us-cert.cisa.gov text/html	MISC us-cert.cisa.gov/ics/advisories/icsa-20-287-05
	Vendor Advisory cert-portal.siemens.com application/pdf	MISC cert-portal.siemens.com/productcert/pdf/ssa-226339.pdf

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Siemens	Desigo Insight	All	All	All	All
Application	Siemens	Desigo Insight	6.0	-	All	All
Application	Siemens	Desigo Insight	6.0	sp2	All	All
Application	Siemens	Desigo Insight	6.0	sp3	All	All
Application	Siemens	Desigo Insight	6.0	sp5	All	All
Application	Siemens	Desigo Insight	All	All	All	All
Application	Siemens	Desigo Insight	6.0	-	All	All
Application	Siemens	Desigo Insight	6.0	sp2	All	All
Application	Siemens	Desigo Insight	6.0	sp3	All	All
Application	Siemens	Desigo Insight	6.0	sp5	All	All

cpe:2.3:a:siemens:desigo_insight:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_insight:6.0:-:*:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_insight:6.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_insight:6.0:sp3:*:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_insight:6.0:sp5:*:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_insight:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_insight:6.0:-:*:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_insight:6.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_insight:6.0:sp3:*:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_insight:6.0:sp5:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report