



CVE-2021-37181

Published on: 09/14/2021 12:00:00 AM UTC

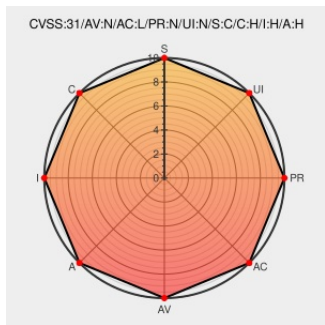
Last Modified on: 09/24/2021 03:20:00 PM UTC

CVE-2021-37181

Source: Mitre

Source: Nist

Print: PDF



Certain versions of [Cerberus Dms](#) from [Siemens](#) contain the following vulnerability:

A vulnerability has been identified in Cerberus DMS V4.0 (All versions), Cerberus DMS V4.1 (All versions), Cerberus DMS V4.2 (All versions), Cerberus DMS V5.0 (All versions < v5.0 QU1), Desigo CC Compact V4.0 (All versions), Desigo CC Compact V4.1 (All versions), Desigo CC Compact V4.2 (All versions), Desigo CC Compact V5.0 (All versions < V5.0 QU1), Desigo CC V4.0 (All versions), Desigo CC V4.1 (All versions), Desigo CC V4.2 (All versions), Desigo CC V5.0 (All versions < V5.0 QU1). 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.

CVE-2021-37181 has been assigned by [S](#) productcert@siemens.com to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: 10 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
	cert-portal.siemens.com/application/pdf	S MISC cert-portal.siemens.com/productcert/pdf/ssa-453715.pdf

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Siemens	Cerberus Dms	4.0	All	All	All
Application	Siemens	Cerberus Dms	4.1	All	All	All
Application	Siemens	Cerberus Dms	4.2	All	All	All
Application	Siemens	Cerberus Dms	5.0	-	All	All
Application	Siemens	Desigo Cc	4.0	All	All	All
Application	Siemens	Desigo Cc	4.1	All	All	All
Application	Siemens	Desigo Cc	4.2	All	All	All
Application	Siemens	Desigo Cc	5.0	-	All	All
Application	Siemens	Desigo Cc Compact	4.0	All	All	All
Application	Siemens	Desigo Cc Compact	4.1	All	All	All
Application	Siemens	Desigo Cc Compact	4.2	All	All	All
Application	Siemens	Desigo Cc Compact	5.0	-	All	All

cpe:2.3:a:siemens:cerberus_dms:4.0:*:*:*:*:*:

cpe:2.3:a:siemens:cerberus_dms:4.1:*:*:*:*:*:

cpe:2.3:a:siemens:cerberus_dms:4.2:*:*:*:*:*:

cpe:2.3:a:siemens:cerberus_dms:5.0:-:*:*:*:*:

cpe:2.3:a:siemens:desigo_cc:4.0:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_cc:4.1:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_cc:4.2:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_cc:5.0:-:*:*:*:*:

cpe:2.3:a:siemens:desigo_cc_compact:4.0:*:*:*:*:*:


cpe:2.3:a:siemens:desigo_cc_compact:4.1:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_cc_compact:4.2:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_cc_compact:5.0:-:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVereport	CVE-2021-37181 : A vulnerability has been identified in Cerberus DMS V4.0 All versions , Cerberus DMS V4.1 All ve... twitter.com/i/web/status/1...	2021-09-14 10:59:48

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2021   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)