



CVE-2021-40354

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

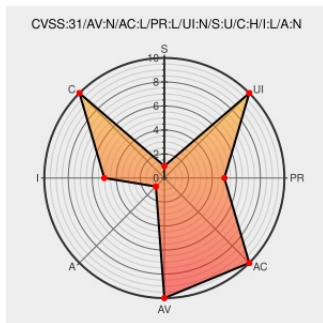
Last Modified on: 09/28/2021 01:15:00 PM UTC

CVE-2021-40354

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)



Certain versions of [Teamcenter Visualization](#) from [Siemens](#) contain the following vulnerability:

A vulnerability has been identified in Teamcenter V12.4 (All versions < V12.4.0.8), Teamcenter V13.0 (All versions < V13.0.0.7), Teamcenter V13.1 (All versions < V13.1.0.5), Teamcenter V13.2 (All versions < 13.2.0.2). The "surrogate" functionality on the user profile of the application does not perform sufficient access control that could lead to an account takeover. Any profile on the application can perform this attack and access any other user assigned tasks via the "inbox/surrogate tasks".

an account takeover. Any profile on the application can perform this attack and access any other user assigned tasks via the "inbox/surrogate tasks".

CVE-2021-40354 has been assigned by [S](#) productcert@siemens.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [S](#) **Siemens** - **Teamcenter V12.4** version **All versions < V12.4.0.8**

Affected Vendor/Software: [S](#) **Siemens** - **Teamcenter V13.0** version **All versions < V13.0.0.7**

Affected Vendor/Software: [S](#) **Siemens** - **Teamcenter V13.1** version **All versions < V13.1.0.5**

Affected Vendor/Software: [S](#) **Siemens** - **Teamcenter V13.2** version **All versions < 13.2.0.2**

CVSS3 Score: **7.1 - HIGH**

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

CVSS2 Score: **5.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality	Integrity	Availability

Impact	Impact	Impact
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
	cert-portal.siemens.com application/pdf	S MISC cert-portal.siemens.com/productcert/pdf/ssa-987403.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	Teamcenter Visualization	All	All	All	All

```
cpe:2.3:a:siemens:teamcenter_visualization:****:*:*:*:*:
```

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-40354 : A vulnerability has been identified in Teamcenter V12.4 All versions < V12.4.0.8 , Teamcenter V13... twitter.com/i/web/status/1...	2021-09-14 11:04:16

← Previous ID

Next ID →

© CVE.report 2021 [Twitter](#) [LinkedIn](#) |

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](#)