

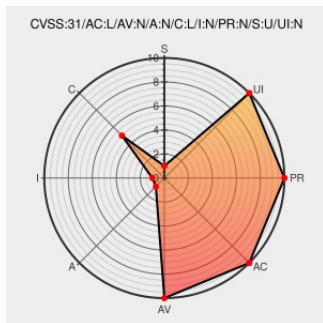


CVE-2020-26178

Published on: 12/18/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:55 PM UTC

CVE-2020-26178

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Business Workflow](#) from [Tangro](#) contain the following vulnerability:

In tangro Business Workflow before 1.18.1, knowing an attachment ID, it is possible to download workitem attachments without being authenticated.

CVE-2020-26178 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
Tangro Software Components GmbH	Product www.tangro.de text/html	t MISC www.tangro.de/
Advisory: Tangro BWF 1.17.5 Multiple Vulnerabilities -	Exploit	to MISC blog.to.com/advisory-tangro-bwf-1-17-5-multiple-

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tangro	Business Workflow	All	All	All	All
Application	Tangro	Business Workflow	All	All	All	All
cpe:2.3:a:tangro:business_workflow:*.*.*.*.*.*.*.*.*.						
cpe:2.3:a:tangro:business_workflow:*.*.*.*.*.*.*.*.*.						

Next ID→