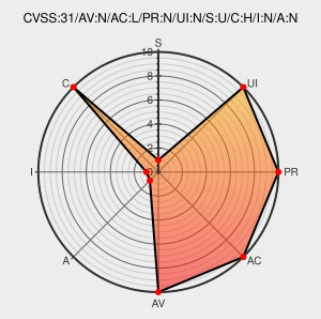
CVE-2020-28054

Published on: 11/19/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-28054

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



Certain versions of Tsmmanager from Tsmmanager contain the following vulnerability:

JamoDat TSMManager Collector version up to 6.5.0.21 is vulnerable to an Authorization Bypass because the Collector component is not properly validating an authenticated session with the Viewer. If the Viewer has been modified (binary patched) and the Bypass Login functionality is being used, an attacker can request every Collector's functionality as if they were a properly logged-in user: administrating connected instances, reviewing logs, editing configurations, accessing the instances' consoles, accessing hardware configurations, etc.Exploiting this vulnerability won't grant an attacker access nor control on remote ISP servers as no credentials is sent with the request.

CVE-2020-28054 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	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
Tivoli Madness - VoidSec	Third Party Advisory voidsec.com text/html	MISC voidsec.com/tivoli-madness/
No Description Provided	Product tsmmanager.com text/html	MISC tsmmanager.com
VoidSec	Third Party Advisory voidsec.com text/html	MISC voidsec.com

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

Exploit/POC from Github

Advisory for CVE-2020-28054 & stack based buffer overflow in IBM Tivoli Storage Manager

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tsmmanager	Tsmmanager	All	All	All	All

cpe:2.3:a:tsmmanager:tsmmanager:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@Attackerkb_Bot	A new #attackerkb assesment on 'CVE-2020-28054' has been created by VoidSec. Attacker Value: 1 | Exploitability: 1 attackerkb.com/assessments/8b…	2021-09-30 14:13:17

← Previous ID

Next ID→