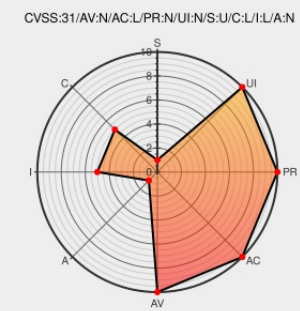
CVE-2023-36857

Published on: Not Yet Published

Last Modified on: 10/25/2023 02:28:00 PM UTC

CVE-2023-36857 - advisory for ICSA-23-269-05

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



Certain versions of Bentley Nevada 3500 System from Bakerhughes contain the following vulnerability:

Baker Hughes – Bently Nevada 3500 System TDI Firmware version 5.05 contains a replay vulnerability which could allow an attacker to replay older captured packets of traffic to the device to gain access.

CVE-2023-36857 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Baker Hughes - Bently Nevada** - **Bently Nevada 3500 System** version **= 5.05**

Vulnerability Patch/Work Around

Baker Hughes – Bently Nevada recommends that users follow their hardening guidelines to reduce the risk of exploitation. Customers who have registered for access to Baker Hughes DAM may directly access the hardening guideline at https://dam.bakerhughes.com/media/?mediaId=32F7FC2F-9F22-4C69-BB847565B7834D08 https://dam.bakerhughes.com/media/ .For customers that do not have access to Baker Hughes DAM may send an email to bentlysupport@bakerhughes.com to request document 106M9733.

CVSS3 Score: 6.5 - MEDIUM

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

CVE References

Description	Tags	Link
Baker Hughes Bently Nevada 3500 | CISA	www.cisa.gov text/html	MISC www.cisa.gov/news-events/ics-advisories/icsa-23-269-05

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
Hardware	Bakerhughes	Bentley Nevada 3500 System	-	All	All	All
Operating System	Bakerhughes	Bentley Nevada 3500 System Firmware	5.0.5	All	All	All

cpe:2.3:h:bakerhughes:bentley_nevada_3500_system:-:*:*:*:*:*:*:*:

cpe:2.3:o:bakerhughes:bentley_nevada_3500_system_firmware:5.0.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→