



CVE-2022-29952

Published on: Not Yet Published

Last Modified on: 08/02/2022 08:53:00 PM UTC

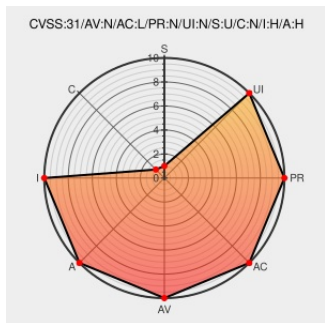
CVE-2022-29952

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Bently Nevada 3701/40](#) from [Bakerhughes](#) contain the following vulnerability:

Bently Nevada condition monitoring equipment through 2022-04-29 mishandles authentication. It utilizes the TDI command and data protocols (60005/TCP, 60007/TCP) for communications between the monitoring controller and System 1 and/or Bently Nevada Monitor Configuration (BNMC) software. These protocols provide configuration management and historical data related functionality. Neither protocol has any authentication features, allowing any attacker capable of communicating with the ports in question to invoke (a subset of) desired functionality.

CVE-2022-29952 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.1 - CRITICAL**

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

CVE References

Description	Tags	Link
Bently Nevada ADAPT 3701/4X Series and 60M100 CISA	www.cisa.gov text/html	MISC www.cisa.gov/uscert/ics/advisories/icsa-22-188-02
Blog - Forescout	web.archive.org text/html Inactive Link Not Archived	MISC www.forescout.com/blog/

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 warrant the accuracy, completeness, or timeliness of the information provided on these sites. CVEreport is not responsible for any damage or loss resulting from the use of the information provided on these sites.

CVE-report 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	Bently Nevada 3701/40	-	All	All	All
Operating System	Bakerhughes	Bently Nevada 3701/40 Firmware	All	All	All	All
Hardware 	Bakerhughes	Bently Nevada 3701/44	-	All	All	All
Operating System	Bakerhughes	Bently Nevada 3701/44 Firmware	All	All	All	All
Hardware 	Bakerhughes	Bently Nevada 3701/46	-	All	All	All
Operating System	Bakerhughes	Bently Nevada 3701/46 Firmware	All	All	All	All
Hardware 	Bakerhughes	Bently Nevada 60m100	-	All	All	All
Operating System	Bakerhughes	Bently Nevada 60m100 Firmware	-	All	All	All
cpe:2.3:h:bakerhughes:bently_nevada_3701V40:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:bakerhughes:bently_nevada_3701V40_firmware:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:bakerhughes:bently_nevada_3701V44:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:bakerhughes:bently_nevada_3701V44_firmware:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:bakerhughes:bently_nevada_3701V46:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:bakerhughes:bently_nevada_3701V46_firmware:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:bakerhughes:bently_nevada_60m100:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:bakerhughes:bently_nevada_60m100_firmware:-:~::~~::~~::~~::~~::~~::~~:::						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-29952 : Bently Nevada condition monitoring equipment through 2022-04-29 mishandles authentication. It util... twitter.com/i/web/status/1...	2022-07-26 22:09:14
 /r/netcve	CVE-2022-29952	2022-07-26 22:38:18

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023  |

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](#)