



CVE-2021-46576

Published on: Not Yet Published

Last Modified on: 02/28/2022 05:50:05 PM UTC

CVE-2021-46576

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

Certain versions of [Microstation](#) from [Bentley](#) contain the following vulnerability:

This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15370.

CVE-2021-46576 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Bentley - MicroStation CONNECT** version **10.16.0.80**

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
BE-2021-0005: Out-of-bounds and use-after-free vulnerabilities in MicroStation and MicroStation-based applications	Vendor Advisory www.bentley.com text/html	B MISC www.bentley.com/en/common-vulnerability-exposure/BE-2021-0005
ZDI-22-163 Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	Z MISC www.zerodayinitiative.com/advisories/ZDI-22-163/

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	Bentley	Microstation	All	All	All	All
Application	Bentley	Microstation Connect	10.16.0.80	All	All	All
Application	Bentley	View	All	All	All	All
cpe:2.3:a:bentley:microstation:*:*:*:*:*:						
cpe:2.3:a:bentley:microstation_connect:10.16.0.80:*:*:*:*:						
cpe:2.3:a:bentley:view:*:*:*:*:*:						

Discovery Credit
Mat Powell of Trend Micro Zero Day Initiative

Social Mentions		
Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-46576 : This vulnerability allows remote attackers to execute arbitrary code on affected installations of... twitter.com/i/web/status/1...	2022-03-01 00:14:24

