

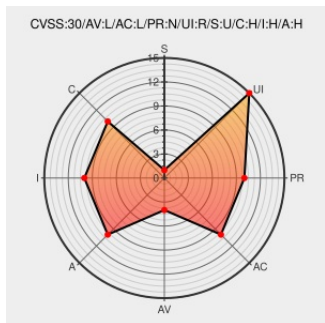


CVE-2021-34896

Published on: 01/13/2022 12:00:00 AM UTC

Last Modified on: 01/14/2022 09:39:00 PM UTC

CVE-2021-34896

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

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

This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 BMP files. The issue results from the lack of proper

validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14863.

CVE-2021-34896 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Bentley - View** version **10.15.0.75**

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
ZDI-21-1485 Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-21-1485/
BE-2021-0002: Out-of-bounds vulnerabilities in MicroStation and MicroStation-based applications	www.bentley.com text/html	MISC www.bentley.com/en/common-vulnerability-exposure/BE-2021-0002

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	Bentley View	All	All	All	All
Application	Bentley	Microstation	All	All	All	All

cpe:2.3:a:bentley:bentley_view:*:*:*:*:*:

cpe:2.3:a:bentley:microstation:*:*:*:*:*:

Discovery Credit

Mat Powell of Trend Micro Zero Day Initiative

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-34896 : This vulnerability allows remote attackers to execute arbitrary code on affected installations of... twitter.com/i/web/status/1...	2022-01-13 22:02:18

← Previous ID

Next ID →