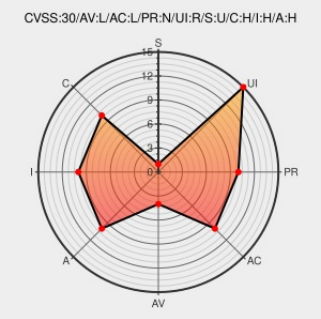
CVE-2022-28305

Published on: Not Yet Published

Last Modified on: 04/05/2023 02:04:00 PM UTC

CVE-2022-28305

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 10.16.02.034. 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 OBJ files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16172.

CVE-2022-28305 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Bentley** - **MicroStation CONNECT** version **10.16.02.034**

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

CVE References

Description	Tags	Link
BE-2022-0008: OBJ File Parsing Stack Overflow vulnerabilities in MicroStation and MicroStation-based applications	web.archive.org text/html Inactive Link Not Archived	MISC www.bentley.com/en/common-vulnerability-exposure/be-2022-0008
ZDI-22-593 | Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-22-593/

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	View	All	All	All	All

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

cpe:2.3:a:bentley:view:*:*:*:*:*:*:*:*:

Discovery Credit

Anonymous

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-28305 : This vulnerability allows remote attackers to execute arbitrary code on affected installations of… twitter.com/i/web/status/1…	2023-03-29 19:02:28

← Previous ID

Next ID→