



# CVE-2022-1229

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2022-1229
<b>State</b>	PUBLIC
<b>Assigner</b>	zdi-disclosures@trendmicro.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-03-28 19:15:00 UTC
<b>Updated</b>	2023-04-04 16:24:00 UTC
<b>Description</b>	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNE

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bentley	Microstation Connect	10.16.2.034	All	All	All

## References

Reference	Source	Link
BE-2022-0006: IFC File Parsing Vulnerabilities in MicroStation and MicroStation-based applications	MISC	<a href="http://www.bentley.com">www.bentley.com</a>
ZDI-22-615   Zero Day Initiative	MISC	<a href="http://www.zerodayinitiative.com">www.zerodayinitiative.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)