



CVE-2023-25002

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2023-25002
State	PUBLIC
Assigner	psirt@autodesk.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-27 23:15:00 UTC
Updated	2023-07-06 16:13:00 UTC
Description	A maliciously crafted SKP file in Autodesk products is used to trigger use-after-free vulnerability. Exploitation of this vulnera

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Autodesk	3ds Max	2022	All	All	All
Application	Autodesk	3ds Max	2023	All	All	All
Application	Autodesk	Navisworks	2022	All	All	All
Application	Autodesk	Navisworks	2023	All	All	All
Application	Autodesk	Revit	2022	All	All	All
Application	Autodesk	Revit	2023	All	All	All
Application	Autodesk	Vred	2023	All	All	All

References

Reference	Source	Link	Tags
adsk-sa-2023-0002	MISC	www.autodesk.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

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](#)