



CVE-2023-35031

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2023-35031
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-12 02:15:00 UTC
Updated	2023-06-20 19:15:00 UTC
Description	Atos Unify OpenScape 4000 Assistant V10 R1 before V10 R1.42.0 and V10 R1.34.8, Assistant V10 R0, Manager V10 R1 b

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atos	Unify Openscape 4000 Assistant	10	r0	All	All
Application	Atos	Unify Openscape 4000 Assistant	10	r1	All	All
Application	Atos	Unify Openscape 4000 Assistant	10	r1.34.4	All	All
Application	Atos	Unify Openscape 4000 Manager	10	r0	All	All
Application	Atos	Unify Openscape 4000 Manager	10	r1	All	All
Application	Atos	Unify Openscape 4000 Manager	10	r1.34.4	All	All

References

Reference

networks.unify.com/security/advisories/OBSO-2305-01.pdf

Unify OpenScape 4000 gefährdet: Neue Sicherheitslücke! Mehrere Schwachstelle ermöglicht Ausführen von beliebigem Programmcode | new

CVE Program record

NVD vulnerability detail

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](#)