



CVE-2022-31216

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

Summary

CVE	CVE-2022-31216
State	PUBLIC
Assigner	cybersecurity@ch.abb.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-15 19:15:00 UTC
Updated	2023-09-13 04:15:00 UTC
Description	Vulnerabilities in the Drive Composer allow a low privileged attacker to create and write to a file anywhere on the file system

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Abb	Automation Builder	All	All	All	All
Application	Abb	Drive Composer	All	All	All	All
Application	Abb	Drive Composer	All	All	All	All
Application	Abb	Mint Workbench	All	All	All	All

References

Reference	Source	Link	Tags
search.abb.com/library/Download.aspx	MISC	search.abb.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.

Legacy QID Mappings

[591008](#) ABB Drive Composer, Automation Builder, Mint Workbench Multiple Vulnerabilities (ICSA-22-202-01) (ABBVREP0072)

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report