



CVE-2021-26262

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

Summary

CVE	CVE-2021-26262
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-19 19:15:00 UTC
Updated	2022-08-01 12:33:00 UTC
Description	Philips MRI 1.5T and MRI 3T Version 5.x.x does not restrict or incorrectly restricts access to a resource from an unauthoriz

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Philips	Mri 1.5t	-	All	All	All
Operating System	Philips	Mri 1.5t Firmware	All	All	All	All
Hardware	Philips	Mri 3t	-	All	All	All
Operating System	Philips	Mri 3t Firmware	All	All	All	All

References

Reference	Source	Link	Tags
Philips MRI 1.5T and 3T CISA	MISC	us-cert.cisa.gov	
Product Security Philips	MISC	www.usa.philips.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Michael Aguilar, a Secureworks Adversary Group consultant, reported these vulnerabilities to Philips.

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](#)