Philips MRI 1.5T and 3T Information Exposure

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-42744
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-19 19:15:09 UTC
Updated	2026-04-02 14:16:21 UTC
Description	Philips MRI 1.5T and MRI 3T Version 5.3 through 5.8.1 does not restrict or incorrectly restricts access to a resource from ar

Risk And Classification

Primary CVSS: v4.0 5.9 MEDIUM from 20705f08-db8b-4497-8f94-7eea62317651

CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-552 | NVD-CWE-noinfo | CWE-552 CWE-552 Files or directories accessible to external parties

Version	Source	Type	Score	Severity	Vector
4.0	20705f08-db8b-4497-8f94-7eea62317651	Secondary	5.9	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:
4.0	CNA	CVSS	5.9	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:
3.1	nvd@nist.gov	Primary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
2.0	nvd@nist.gov	Primary	2.1		AV:L/AC:L/Au:N/C:P/I:N/A:N

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

ntegrity

None

Availability

None

AV:L/AC:L/Au:N/C:P/I:N/A:N

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Philips	MRI 1.5T	affected 5.3 5.8.1 custom	Not specified
CNA	Philips	MRI 3T	affected 5.3 5.8.1 custom	Not specified

References

Reference	Source	Link	Tags
Philips MRI 1.5T and 3T | CISA	af854a3a-2127-422b-91ae-364da2661108	us-cert.cisa.gov	Third Party Advisory, US Government
Product Security | Philips	af854a3a-2127-422b-91ae-364da2661108	www.usa.philips.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Michael Aguilar, a Secureworks Adversary Group consultant, reported these vulnerabilities to Philips. (en)

Additional Advisory Data

Workarounds

CNA: Philips released a software upgrade version 5.8.2 to remediate these vulnerabilities and can be referenced by FCO78100619. As an interim mitigation to these vulnerabilities, Philips recommends the following: Users should operate all Philips deployed and supported products within Philips authorized specifications, including physical and logical controls. Only allowed

personnel are permitted in the vicinity of the product. Refer to the Philips instructions for use (IFU) available on InCenter https://incenter.medical.philips.com. Users with questions about their specific MRI product should contact a Philips service support team or regional service support. Philips contact information is available at the Philips customer service solutions website http://philips.com/productsecurity or by calling 1-800-722-9377. For more information regarding these vulnerabilities, see the Philips product security advisory website http://philips.com/productsecurity. Users can also visit the Philips product security website for the latest security information for Philips products.

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