



CVE-2020-9476

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

Summary

CVE	CVE-2020-9476
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-04 19:15:00 UTC
Updated	2023-11-07 03:26:00 UTC
Description	ARRIS TG1692A devices allow remote attackers to discover the administrator login name and password by reading the /log

Risk And Classification

Problem Types: CWE-326

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Commscope	Arris Tg1692a	-	All	All	All
Hardware	Commscope	Arris Tg1692a	-	All	All	All
Operating System	Commscope	Arris Tg1692a Firmware	9.1.103de2	All	All	All
Operating System	Commscope	Arris Tg1692a Firmware	9.1.103de2	All	All	All

References

Reference	Source	Link	Ti
Info disclosure — CVE-2020-9476. The Arris tg1692a router firmware... by Rafael Silva Medium	MISC	medium.com	E
Info disclosure — CVE-2020-9476. The Arris tg1692a router firmware... by Rafael Silva Medium		medium.com	
ARRIS Consumer Care - Support Services	MISC	arris.secure.force.com	V
CVE Program record	CVE.ORG	www.cve.org	ce
NVD vulnerability detail	NVD	nvd.nist.gov	ce

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](#)