



CVE-2020-29138

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

Summary

CVE	CVE-2020-29138
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-27 16:15:00 UTC
Updated	2023-11-07 03:21:00 UTC
Description	Incorrect Access Control in the configuration backup path in SAGEMCOM F@ST3486 NET DOCSIS 3.0, software NET_4.1

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Sagemcom	F@st 3486 Router	3.0	All	All	All
Hardware	Sagemcom	F@st 3486 Router	3.0	All	All	All
Operating System	Sagemcom	F@st 3486 Router Firmware	4.109.0	All	All	All
Operating System	Sagemcom	F@st 3486 Router Firmware	4.109.0	All	All	All

References

Reference
Medium
CVE 2020-29138 — Improper Access Control in the SAGEMCOM router, model F@ST 3486 running NET_4.109.0 by Alexandre Vieira No
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](#)