



CVE-2021-3304

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

Summary

CVE	CVE-2021-3304
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-26 18:16:00 UTC
Updated	2021-02-03 15:57:00 UTC
Description	Sagemcom F@ST 3686 v2 3.495 devices have a buffer overflow via a long sessionKey to the goform/login URI.

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Sagemcom	F@st 3686	v2	All	All	All
Hardware	Sagemcom	F@st 3686	v2	All	All	All
Hardware	Sagemcom	F@st 3686	v2	All	All	All
Operating System	Sagemcom	F@st 3686 Firmware	3.495	All	All	All
Operating System	Sagemcom	F@st 3686 Firmware	3.495	All	All	All

References

Reference

jonhat auf Twitter: "Sagemcom F@ST3686 buf overflow. Reported 4 months ago, no fix. Mitigate by changing default IPs & remote management"

[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.

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](#)