CVE-2019-7438

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2019-7438
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-21 16:01:00 UTC
Updated	2019-04-26 14:24:00 UTC
Description	cgi-bin/qcmap_web_cgi on JioFi 4G M2S 1.0.2 devices has XSS and HTML injection via the mask POST parameter.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Jio	Jiofi 4g M2s	-	All	All	All
Hardware	Jio	Jiofi 4g M2s	-	All	All	All
Operating System	Jio	Jiofi 4g M2s Firmware	1.0.2	All	All	All
Operating System	Jio	Jiofi 4g M2s Firmware	1.0.2	All	All	All

References

Reference	Source
JioFi 4G M2S 1.0.2 - 'mask' Cross-Site Scripting - Hardware webapps Exploit	EXPLO
cgi-bin/qcmap_web_cgi on JioFi 4G M2S 1.0.2 devices has HTML injection via the mask POST parameter-CVE-2019-7438 (HTML)	MISC
cgi-bin/qcmap_web_cgi on JioFi 4G M2S 1.0.2 devices has XSS via the mask POST parameter-CVE-2019-7438 (XSS)	MISC
JioFi 4G M2S 1.0.2 Cross Site Scripting ≈ Packet Storm	MISC
CVE Program record	CVE.OI
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report