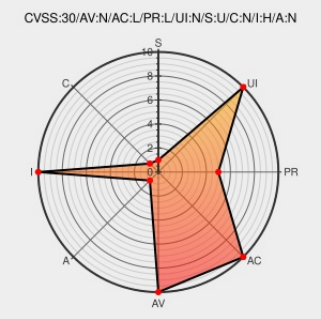
CVE-2017-10718

Published on: 06/17/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:28 PM UTC

CVE-2017-10718

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Endoscope Camera from Ishekar contain the following vulnerability:

Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that any malicious user connecting to the device can change the default SSID and password thereby denying the owner an access to his/her own device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.

CVE-2017-10718 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
IoT_vulnerabilities/Shekar_boriscope_sec_issues.pdf at master · ethanhunnt/IoT_vulnerabilities · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/ethanhunnt/IoT_vulnerabilities/blob/master/Shek
Shekar Endoscope Weak Default Settings / Memory Corruption ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/153241/Shekar-End Settings-Memory-Corruption.html
Bugtraq: Newly releases IoT security issues	Mailing List Third Party Advisory seclists.org text/html	BUGTRAQ 20190609 Newly releases IoT security issues

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Ishekar	Endoscope Camera	-	All	All	All
Hardware	Ishekar	Endoscope Camera	-	All	All	All
Operating System	Ishekar	Endoscope Camera Firmware	All	All	All	All
Operating System	Ishekar	Endoscope Camera Firmware	All	All	All	All

cpe:2.3:h:ishekar:endoscope_camera:-:*:*:*:*:*:*:*:

cpe:2.3:h:ishekar:endoscope_camera:-:*:*:*:*:*:*:*:

cpe:2.3:o:ishekar:endoscope_camera_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:ishekar:endoscope_camera_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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