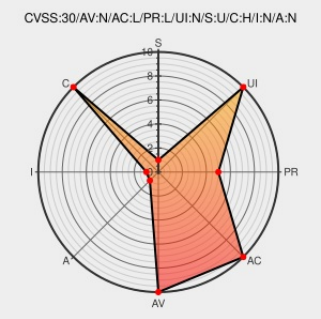
CVE-2017-10719

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

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

CVE-2017-10719

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 the device has default Wi-Fi credentials that are exactly the same for every 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-2017-10719 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	HIGH	NONE	NONE

CVSS2 Score: 4 - MEDIUM

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

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→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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