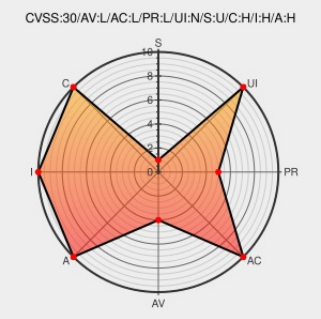
CVE-2017-10720

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

Last Modified on: 03/23/2021 11:26:27 PM UTC

CVE-2017-10720

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 desktop application used to connect to the device suffers from a stack overflow if more than 26 characters are passed to it as the Wi-Fi name. This application is installed on the device and an attacker who can provide the right payload can execute code on the user's system directly. Any breach of this system can allow an attacker to get access to all the data that the user has access too. The application uses a dynamic link library(DLL) called "avilib.dll" which is used by the application to send binary packets to the device that allow to control the device. One such action that the DLL provides is change password in the function "sendchangename" which allows a user to change the Wi-Fi name on the device. This function calls a sub function "sub_75876EA0" at address 0x758784F8. The function determines which action to execute based on the parameters sent to it. The "sendchangename" passes the datastring as the second argument which is the name we enter in the textbox and integer 1 as first argument. The rest of the 3 arguments are set to 0. The function "sub_75876EA0" at address 0x75876F19 uses the first argument received and to determine which block to jump to. Since the argument passed is 1, it jumps to 0x75876F20 and proceeds from there to address 0x75876F56 which calculates the length of the data string passed as the first parameter. This length and the first argument are then passed to the address 0x75877001 which calls the memmove function which uses a stack address as the destination where the password typed by us is passed as the source and length calculated above is passed as the number of bytes to copy which leads to a stack overflow.

CVE-2017-10720 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE

Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

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→