



CVE-2020-10513

Published on: 04/15/2020 12:00:00 AM UTC

Last Modified on: 05/03/2022 02:06:00 PM UTC

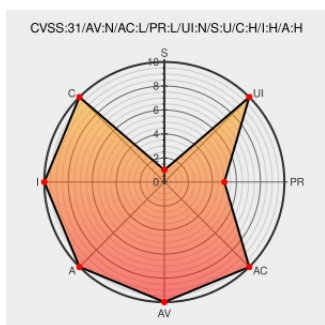
CVE-2020-10513

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Dvr Interface](#) from [Icatchinc](#) contain the following vulnerability:

The file management interface of iCatch DVR firmware before 20200103 contains broken access control which allows the attacker to remotely manipulate arbitrary file.

CVE-2020-10513 has been assigned by [cve@cert.org.tw](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [iCatch Inc.](#) - **DVR firmware** version **before 20200103**

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
TWCERT/CC台灣電腦網路危機處理暨協調中心-資安服務-台灣漏洞揭露平台 (TVN)-TVN (Taiwan Vulnerability Note) 漏洞公告-iCatch DVR產品 - Broken Access Control	Third Party Advisory www.twcert.org.tw text/html	MISC www.twcert.org.tw/tw/cp-132-3533-10afe-1.html

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Icatchinc	Dvr Interface	All	All	All	All
Application	Icatchinc	Dvr Interface	All	All	All	All
cpe:2.3:a:icatchinc:dvr_interface:*. *.*.*.*.*.*:						
cpe:2.3:a:icatchinc:dvr_interface:*. *.*.*.*.*.*:						

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------