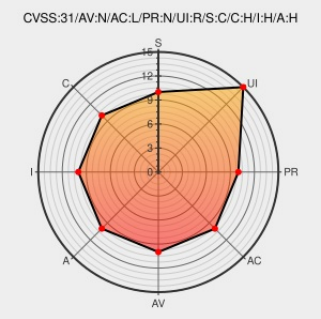
CVE-2020-14498

Published on: 08/26/2020 12:00:00 AM UTC

Last Modified on: 09/23/2021 01:34:00 PM UTC

CVE-2020-14498 - advisory for ICSA-20-210-03

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



Certain versions of Ecatcher from Hms-networks contain the following vulnerability:

HMS Industrial Networks AB eCatcher all versions prior to 6.5.5. The affected product is vulnerable to a stack-based buffer overflow, which may allow an attacker to remotely execute arbitrary code.

CVE-2020-14498 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **HMS Industrial Networks AB** - **eCatcher** version **< 6.5.5**

CVSS3 Score: 10 - CRITICAL

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

CVSS2 Score: 10 - HIGH

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

CVE References

Description	Tags	Link
HMS Industrial Networks eCatcher | CISA	Third Party Advisory US Government Resource us-cert.cisa.gov	MISC us-cert.cisa.gov/ics/advisories/icsa-20-210-03

text/html

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
Application	Hms-networks	Ecatcher	All	All	All	All
Application	Hms-networks	Ecatcher	All	All	All	All

cpe:2.3:a:hms-networks:ecatcher:*:*:*:*:*:*:*:*:

cpe:2.3:a:hms-networks:ecatcher:*:*:*:*:*:*:*:*:

Discovery Credit

Sharon Brizinov of Claroty reported this vulnerability to CISA.

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

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