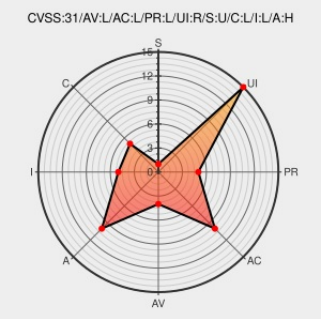
CVE-2021-33214

Published on: 07/09/2021 12:00:00 AM UTC

Last Modified on: 09/21/2021 04:33:00 PM UTC

CVE-2021-33214

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



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

In HMS Ewon eCatcher through 6.6.4, weak filesystem permissions could allow malicious users to access files that could lead to sensitive information disclosure, modification of configuration files, or disruption of normal system operation.

CVE-2021-33214 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	LOW	HIGH

CVSS2 Score: 6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
eCatcher Desktop — Version 6.6.4	labs.bishopfox.com text/html	MISC labs.bishopfox.com/advisories/ecatcher-desktop-version-6.6.4
Advisories	labs.bishopfox.com text/html	MISC labs.bishopfox.com/advisories

Security at every level of our solution	www.ewon.biz text/html	MISC www.ewon.biz/about-us/security
eCatcher	www.ewon.biz text/html	MISC www.ewon.biz/technical-support/pages/talk2m/talk2m-tools/talk2m-ecatcher
	cdn.hms-networks.com application/pdf	MISC cdn.hms-networks.com/docs/librariesprovider6/cybersecurity/hms-security-advisory-2021-07-09-001---ewon-ecatcher.pdf?sfvrsn=b37418d7_4

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-33214 : In HMS Ewon eCatcher through 6.6.4, weak filesystem permissions could allow malicious users to acc… twitter.com/i/web/status/1…	2021-07-09 18:43:45
@threatmeter	HMS Ewon eCatcher up to 6.6.4/6.7.2 permission [CVE-2021-33214] A vulnerability was found in HMS Ewon eCatcher up t… twitter.com/i/web/status/1…	2021-07-11 07:54:22
/r/netcve	CVE-2021-33214	2021-07-09 19:41:54

← Previous ID

Next ID→