



CVE-2020-17475

Published on: 08/14/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:30 PM UTC

CVE-2020-17475

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Koala](#) from [Megvii](#) contain the following vulnerability:

Lack of authentication in the network relays used in MEGVII Koala 2.9.1-c3s allows attackers to grant physical access to anyone by sending packet data to UDP port 5000.

CVE-2020-17475 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
Megvii Koala 2.9.1-c3s architectural vulnerability on network relays - Threat Encyclopedia	Third Party Advisory www.trendmicro.com/text/html	MISC www.trendmicro.com/vinfo/us/threat-encyclopedia/vulnerability/8137/megvii-koala-291c3s-architectural-vulnerability-on-network-relays

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
Hardware 	Megvii	Koala	-	All	All	All
Hardware 	Megvii	Koala	-	All	All	All
Operating System	Megvii	Koala Firmware	2.9.1-c3s	All	All	All
Operating System	Megvii	Koala Firmware	2.9.1-c3s	All	All	All
<code>cpe:2.3:h:megvii:koala:-:*:*:*:*:*:</code>						
<code>cpe:2.3:h:megvii:koala:-:*:*:*:*:*:</code>						
<code>cpe:2.3:o:megvii:koala_firmware:2.9.1-c3s:*:*:*:*:*:</code>						
<code>cpe:2.3:o:megvii:koala_firmware:2.9.1-c3s:*:*:*:*:*:</code>						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)