

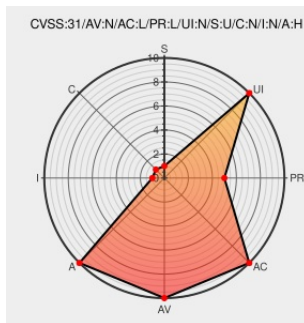


CVE-2020-28349

Published on: 11/08/2020 12:00:00 AM UTC

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

CVE-2020-28349

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

Certain versions of [Network Server](#) from [Chirpstack](#) contain the following vulnerability:

**** DISPUTED **** An inaccurate frame deduplication process in ChirpStack Network Server 3.9.0 allows a malicious gateway to perform uplink Denial of Service via malformed frequency attributes in CollectAndCallOnceCollect in internal/uplink/collect.go. NOTE: the vendor's position is that there are no "guarantees that allowing untrusted LoRa gateways to the network should still result in a secure network."

CVE-2020-28349 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

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	NONE	HIGH

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
LoRaWAN & MQTT: What to Know When Securing Your IoT Network	Exploit Third Party Advisory	MISC www.cyberark.com/resources/threat-research-blog/lorawan-mqtt-what-to-know-when-securing-your-iot-

[www.cyberark.com](#)[network](#)

[text/html](#)

Improve error handling of unknown gateways. · brocaar/chirpstack-network-server@874fc1a · GitHub

[Patch](#)[Third Party Advisory](#)[github.com](#)[text/html](#)

[MISC github.com/brocaar/chirpstack-network-server/commit/874fc1a9b01045ebe8a340f0bb01ed19e8256e60](#)

Improve uplink de-duplication. · brocaar/chirpstack-network-server@f996bb0 · GitHub

[Patch](#)[Third Party Advisory](#)[github.com](#)[text/html](#)

[MISC github.com/brocaar/chirpstack-network-server/commit/f996bb0c6c85281b5658f59ff09db1b4a73db453](#)

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	Chirpstack	Network Server	3.9.0	All	All	All
Application	Chirpstack	Network Server	3.9.0	All	All	All

cpe:2.3:a:chirpstack:network_server:3.9.0:*****:

cpe:2.3:a:chirpstack:network_server:3.9.0:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)