



CVE-2020-28371

Published on: 11/09/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-28371

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Avian](#) from [Readytalk](#) contain the following vulnerability:

**** UNSUPPORTED WHEN ASSIGNED **** An issue was discovered in ReadyTalk Avian 1.2.0 before 2020-10-27. The `FileOutputStream.write()` method in `FileOutputStream.java` has a boundary check to prevent out-of-bounds memory read/write operations. However, an integer overflow leads to bypassing this check and achieving the out-of-bounds access. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.

CVE-2020-28371 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
Fix integer overflow leading	CVE	MISC

Fix integer overflow leading to out-of-bounds read/write · ReadyTalk/avian@0871979 · GitHub

Patch

Third Party Advisory

github.com

text/html

MISC

github.com/ReadyTalk/avian/commit/0871979b298add320ca63f65060acb7532c8a0dd

Fix integer overflow leading to out-of-bounds read/write by polivar3 · Pull Request #572 · ReadyTalk/avian · GitHub

Patch

Third Party Advisory

github.com

text/html

MISC

github.com/ReadyTalk/avian/pull/572

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	Readytalk	Avian	1.2.0	All	All	All
Application	Readytalk	Avian	1.2.0	All	All	All
cpe:2.3:a:readytalk:avian:1.2.0:*:*:*:*:*:						
cpe:2.3:a:readytalk:avian:1.2.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE