New issue

Jump to bottom

Format String Vulnerability #23

Closed **0roman** opened this issue on Sep 2, 2020 · 3 comments

0roman commented on Sep 2, 2020 • edited

Format String Vulnerability

There is a Format String vulnerability in sdp.cpp line 99.

https://github.com/wireapp/wire-audio-video-signaling/blob/6bd9e51730a80cf527f7f30d7f8d6853fb2d875d/src/peerflow/sdp.c#L99

The function parameter **value** of function sdp_media_set_lattr() is controllable by an attacker and can lead to a format string attack. The function sdp_media_set_lattr() is implemented in media.c of the library re.

The vulnerability is fixed in current Android and iOS Wire Applications.

The vulnerability was exploitable in the Android and iOS Wire Apps at least until Wire Android Version 3.46.890 and iOS Version 3.58. An attacker could crash remote Wire Applications by a call with malformed sdp data, if the remote particpant accepted the call. The vulnerability could potentially lead to remote code execution.

franziskuskiefer commented on Sep 3, 2020

Thanks for reporting. This has indeed been fixed but this repository unfortunately wasn't updated yet.
@wireapp/avs can you make sure that we get a version in here that contains the fixes to `sdp.c` ?

jspittka commented on Sep 3, 2020 Member

Thanks for this report. We are currently working on a big release and will wrap up an update to this open source library including all security updates in the mid October time frame.

jspittka commented on Oct 16, 2020 Member

Thanks again for reporting. The code update has been released and the issue should be fixed. Please let us know in case you still see any problem(s).

jspittka closed this as completed on Oct 16, 2020

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

3 participants