# KrackPlus vulnerability report

May 1, 2018

**Summary**

An adversary can attempt to exploit a vulnerability in the 4-way handshake in WPA2 through jamming and resending the third part of the handshake. This report details whether any of the scanned Android or Linux devices are vulnerable to the pairwise or group version of key reinstallation attacks (KRACK).

The first column contains the mac-addresses of the clients that were scanned. The second and third colums detail whether a device was vulnerable to either the pairwise or group version of KRACK.

Pairwise: client seems vulnerable to pairwise key reinstallation in the 4-way handshake (using standard attack).
Group: client is vulnerable to group key reinstallations in the 4-way handshake (or client accepts replayed broadcast frames)

**Device results**

| | None | Parwise | Group |
|---|---|---|---|
| aaaa.aaaa.aaaa.6666: | x | | |
| aaaa.aaaa.aaaa.8888: | | x | |
| aaaa.aaaa.aaaa.2222: | | | x |
| aaaa.aaaa.aaaa.3333: | | x | |
| aaaa.aaaa.aaaa.9999: | | x | |
| aaaa.aaaa.aaaa.7777: | | | x |
| aaaa.aaaa.aaaa.4444: | x | | |
| aaaa.aaaa.aaaa.1111: | x | | |
| aaaa.aaaa.aaaa.5555: | | x | x |