WPA Security Vulnerability

On October 16, 2017 an issue with the implementation of the 4-way handshake used to establish security in wireless networks was disclosed.

What is the Issue?

When connecting to a wireless network protected with WPA/WPA2, a 4-way handshake is used to establish a per-device temporary cryptographic key to protect transmissions. The 4-way handshake itself is mathematically proven to be secure, however most implementations of the 4-way handshake were found to be vulnerable to attack. Similar attacks were found to be effective against implementations of the group key handshake and the 802.11r handshake. It is important to emphasize the vulnerability is in the implementation of these items, and that there is no inherent security flaw necessitating WPA2 be redesigned.

Who is affected?

This attack is primarily against client devices. The attack involves forcing a retransmit of the 3 rd step in the 4-way handshake, or injecting retransmits, causing the client device to reset key cryptographic parameters which invalidate certain assumptions that form the basis of the mathematics used to protect wireless transmissions. An attack against 802.11r works on the same principle, however 802.11r is disabled by default on Grandstream APs. The following table illustrates capabilities of an attacker using this family of vulnerabilities against Grandstream clients and access points. 4-Way Handshake and 802.11r cases are weaknesses in the cryptography between the AP and single device, affecting only unicast traffic, while Group Key is a weakness in the cryptography used for broadcast and multicast traffic.

	Replay	**Decrypt**	**Forge**
4-Way Handshake			
TKIP	AP->Client	Client->AP	Client->AP
CCMP	AP->Client	Client->AP	No
802.11r			
TKIP	Client->AP	AP->Client	AP->Client
CCMP	Client->AP	AP->Client	No
Group Key	AP->Client	No	No

It is important to note that a patched client is secure, even if unpatched devices are connected to the same wireless network.

What should you do?

Because this attack is primarily a weakness in the client, you should immediately patch all client devices. Please refer to your device vendor for more details.

Hardening Grandstream Access Points

"Out of the box" Grandstream Access Points are not affected by this issue. This does not mean that vulnerable client devices are protected, only that there is no issue with the Access Point side. Vulnerable clients must still be updated.

The default configuration selects WPA2-CCMP and disables the older and known to be problematic TKIP. Ensure that your access points are still using this setting. Additionally, 802.11r (part of Grandstream's Voice Enterprise feature set) is disabled by default. It is recommended to disable this setting until firmware is available.

If you utilize bridge mode, then the AP becomes vulnerable to the 4-Way handshake issue with the same drawbacks as any other vulnerable client device. A fix is available for this and should be applied immediately. The following table lists patched firmware versions for GWN APs.

Note that the bridge mode feature is not yet available on GWN7600/GWN7600LR, but the vulnerability will already be patched when it becomes available.

Since our other devices act as a client firmware fixes were generated as well, the complete list is below of the devices with a ported fix.

Device / Model	Firmware Version	Release Date
GWN7610	1.0.4.21	10/20
GXP1760W	1.0.1.30	
GXV3240/3275	1.0.3.184	
GAC2500	1.0.3.19	
GVC3200	1.0.3.46	