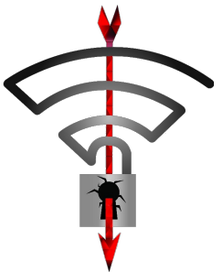
**Jump to: us.comtrend.com/technical-bulletins**

**FOR IMMEDIATE RELEASE**

## Key Reinstallation Attack- WPA2 Vulnerability

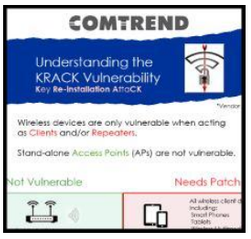


**Models:** Various Wireless (See Below)
**Version:** KRACK_WPA2.V3

**Technical Release Date:** October 31, 2017
**Status:** Varies by Model

## Overview:

The WPA2 vulnerability known as KRACK (Key Reinstallation AttaCK) circumvents standard security on WPA2 protected networks. This vulnerability is being patched by vendors with new software. In simple terms, it affects wireless clients, such as tablets, laptops, smartphones (wireless/not cellular), etc., AND wireless devices acting as clients, such as repeaters and wireless MESH products.



VIEW

Some wireless access points are not vulnerable by default, but ARE vulnerable if 802.11r 'fast roaming' is enabled.

Download the KRACK Infographic for further clarification.

---

## Status

As of today, Tuesday, October 31, 2017, we have determined the following:

- All of our Broadband Provider's Residential Gateways are NOT affected. This includes all products that start with "CT", "NL", "AR", "WR", and "VR".
- Powergrid models PG-9171n and PG-9172AC are also not affected.
- At this time we are assuming any other wireless product that supports "Client" and/or "Repeater" modes will require a patched release. Dates will be announced as soon as possible; those determined by today are below.

The following schedule is our expected release time frames for each model's vulnerability patch.

(* Correction: WR-5882 & WR-5887 will have patches made for client/repeater configuration)

| | | | |
|---|---|---|---|
| **WAP-EN1750C** | 12/2017 | **WAP-5882*** | 2/2018 |
| **WAP-EN1750R** | 12/2017 | **WAP-5883** | 2/2018 |
| **WAP-EN1750W** | 1/2018 | **WAP-5887*** | 2/2018 |
| **WAP-EN1200C** | 1/2018 | **WAP-5920** | 2/2018 |
| **WAP-EN900R** | 1/2018 | **WAP-5930** | 2/2018 |
| **WAP-EN300C** | 1/2018 | **WAP-PC1750W** | 3/2018 |
| **WLC-6404** | 12/2017 | **WAP-PC1200C** | 3/2018 |

---

## Continued Communication

If you would like to receive Comtrend's Technical Bulletins, including updates on this topic, you can sign up here: Comtrend Connection Sign-Up

Our Technical Bulletin & Security updates are also posted at the following location: http://us.comtrend.com/technical-bulletins/

---

## Supplemental Vulnerability Information

Discovered by:  Mathy Vanhoef of imec-DistriNet, KU Leuven via source: https://www.krackattacks.com/#details

---

## Best Practices

Standard procedures of wireless security remain intact, that all wireless devices, including laptops, tablets, smartphones, and computers should be updated to the manufacturer's latest release. CERT-US publishes a list of manufacturers with updates here: http://www.kb.cert.org/vuls/id/228519 (see VU#228519).

---


Your Sales Engineer:

- Gerard.Sison@Comtrend.com, National Accounts & LATAM & Caribbean
- Joseph.Pessy@Comtrend.com, US & Canada
- Walter.Navarro@comtrend.com, US & Canada


We appreciate our technical support community and encourage direct communication with your sales representative and sales engineer contacts above.  If you have any comments or questions about the technical bulletin, our newsletter and/or mailing lists, please email us at comtrendconnection@comtrend.com.



---

**Additional Comtrend Resources**

Early Adopter Program
Customer/Partners aiding in product development

Comtrend YouTube Channel
Support videos and training webinars


www.Comtrend.com 14 Chrysler | Irvine CA 92618 | (949) 753-9640


Join Our Mailing List!