**ADTRAN Security Advisory**

**ID:** ADTSA-KRA1001  
**Key Reinstallation Attack Vulnerability (KRACK)**

**Publication Date:** 2017-10-18

**Affected Products:** Currently investigating. Potentially all ADTRAN Wireless Products

**Summary:** A critical vulnerability has been reported in the WPA2 wireless standard. An attacker within range of a victim can exploit the weaknesses by using a reinstallation key attack to capture and read sensitive information previously thought to be encrypted. This is explained in more detail at [https://www.krackattacks.com/](https://www.krackattacks.com/).

**Solution:** ADTRAN is currently investigating. This document will be updated with information as it becomes available.

**Description:**
The following CVE IDs have been assigned to document these vulnerabilities in the WPA2 protocol:

- **CVE-2017-13077**: Reinstallation of the pairwise key in the Four-way handshake
- **CVE-2017-13078**: Reinstallation of the group key in the Four-way handshake
- **CVE-2017-13079**: Reinstallation of the integrity group key in the Four-way handshake
- **CVE-2017-13080**: Reinstallation of the group key in the Group Key handshake
- **CVE-2017-13081**: Reinstallation of the integrity group key in the Group Key handshake
- **CVE-2017-13082**: Accepting a retransmitted Fast BSS Transition Reassociation Request and reinstalling the pairwise key while processing it
- **CVE-2017-13084**: Reinstallation of the STK key in the PeerKey handshake
- **CVE-2017-13086**: Reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake
- **CVE-2017-13087**: Reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame
- **CVE-2017-13088**: Reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame

**Affected Products:**
ADTRAN is investigating, but potentially all products utilizing WPA2 are affected.

**Impact**
This vulnerability is classified by industry standards as a serious vulnerability. ADTRAN will release security patches for affected products as quickly as possible following the investigation. Since an attacker needs physical proximity to the access point to exploit the weakness, the current recommended action is to monitor this security advisory for further ADTRAN updates that provide additional details on the affected products. Using WEP as an alternative to WPA and WPA2 is strongly discouraged because it is far less secure than WPA2 despite these vulnerabilities.

**Advisory Revisions and Status:**

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Revision Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>2017-10-18</td>
<td>Initial release</td>
</tr>
</tbody>
</table>