ID: ADTSA-BSIM1001   **BSAP Impersonation – upload/execute arbitrary script**   **Revision: A**

Publication Date: 2015-11-16

Affected Products: Bluesocket vWLAN

Summary: An attacker may impersonate a Bluesocket access point and upload/execute arbitrary script.

Solution: Software patches for affected products have been developed and tested.

Description:
A security vulnerability has been identified with the ADTRAN Bluesocket vWLAN and access point products that could potentially allow a remote attacker to impersonate a Bluesocket access point, upload arbitrary script to the Bluesocket vWLAN, and remotely execute that arbitrary script.

How to determine if you are affected:
ADTRAN has determined the following products are impacted:

- Bluesocket vWLAN (all versions)

Impact
A remote attacker could potentially impersonate a Bluesocket access point, upload arbitrary script to the Bluesocket vWLAN, and remotely execute that arbitrary script.

Software Versions and Fixes:

ADTRAN recommends applying the patch in the "Recommended Patch" column to the corresponding release in the "Release" column of the following table:

Product	Release	Recommended Patch
Bluesocket vWLAN 2.6.1 Bluesocket vWLAN 2.5.1	2.6.1.06 2.5.1.07	security-2.6.1.06-1.patch security-2.5.1.07-1.patch

Other Recommendations:
- Replace private keys and certificates.
- If you have installed a 3rd party SSL certificate provided by a CA such as VeriSign on the vWLAN
  - Refer to the "Renewing an SSL Certificate" section of the "Install and Renew SSL Cert vWLAN Version 2.2.1 and Later" guide.
- Change passwords, pre-shared keys and shared secrets
- Place Bluesocket vWLAN behind a firewall and only allow ports/protocols necessary for operation.
  - Refer to AP Discovery Guide for more information on ports and protocols required.

Obtaining Fixed Software:
Software that addresses this vulnerability along with release notes and application instructions will be freely available on the ADTRAN website under Support, Product Downloads, Software Releases, in the Support Community, or customers may obtain assistance under a service plan by opening a technical support case. Please subscribe to software notifications to be alerted when firmware is posted for your product.

Advisory Revisions and Status:

Revision	Date	Type	Status
A	2015-11-16	Initial release	