ADTRAN Security Advisory

ID: ADTSA-HB1001	**OpenSSL – Heartbleed**	**Revision: E**
Publication Date:	2014-05-01	
Affected Products:	Bluesocket vWLAN, NetVanta 1531, ADTRAN Soundpoint & VVX series IP Phones	
Summary:	Remote attackers may obtain potentially sensitive information from process memory.	
Solution:	Software patches for affected products are currently being developed and tested.	

Description:
A potential security vulnerability has recently been announced that impacts systems that utilize certain versions of OpenSSL. The vulnerability, known as "Heartbleed", is officially tracked as CVE-2014-0160. The Heartbleed vulnerability occurs due to the fact that TLS and DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets.

How to determine if you are affected:
ADTRAN is currently working to assess all potential vulnerabilities in its products and solutions. Only products that utilize implementations of OpenSSL 1.0.1 before 1.0.1g are at risk.

The following ADTRAN products are impacted by the "Heartbleed" vulnerability:

- Bluesocket vWLAN (version 2.4 only)
- NetVanta 1531 (version R11.1.0 only)
- ADTRAN Soundpoint series IP phones (321/335/550/650) (UCS versions 4.1.0.84959rts42 to UCS 4.1.6.4835rts50 only)
- ADTRAN VVX series IP phones (300/310/400/410/500/600) (UCS versions 4.1.3.7864rts21G to UCS 5.0.1.7396rts56 Q only)

The following ADTRAN products are NOT impacted by the "Heartbleed" vulnerability:

- ACI-E product series
- Atlas 500 and 800 series
- AOE (Advanced Operational Environment)
- Bluesocket Access Points
- Bluesocket BlueSecure Controllers (BSC)
- Bluesocket vWLAN with software prior to 2.4
- CSU family of products
- hiX 5600 product series
- IP 700 series phones
- MX28xx series
- MX410 and MX412
- N-Command MSP
- N-Command EE
- NetVanta 150 & 160 Access Points
- NetVanta 644 media gateway
- NetVanta 800/8000 series Carrier Ethernet NTEs
- NetVanta 1000 series switches and switch/routers with software R10.11.0 or earlier
- NetVanta 2000 series security appliances
- NetVanta 3000/4000/5000 series routers
- NetVanta 6000 series IP Business Gateways
- NetVanta 7000 series IP Telephony Appliances
- NetVanta Unified Communications Servers (UCS, BCS, ECS and BAS)
- OPTI-3
- OPTI-6100
- Smart 16 systems
- Total Access 300 series Optical Network Terminals (ONT)
- Total Access 600 series Integrated Access Devices
- Total Access 750 series Integrated Access Devices
- Total Access 850 series Integrated Access Devices
- Total Access 900 and 900e series IP Business Gateways
- Total Access 11xx/12xx series Family of Products
- Total Access 14xx series Family of Products
- Total Access 1500 series Family of Products
- Total Access 3000 series Family of Products
- Total Access 4303 series Family of Products
- Total Access 5000 series Family of Products
- Total Access EMS B release series
- Tracer wireless products
- TSU family of products

Impact
This vulnerability allows remote attackers to obtain potentially sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the "Heartbleed" bug.

Temporary Software Workarounds for Affected Products:

- Bluesocket vWLAN (ver. 2.4) – Patches (Heartbleed-TG5986 and RegenerateCerts-TG6350) for software version 2.4 have been posted. See software notification available in the support community at the following url: https://supportforums.adtran.com/message/14003#14003
    - In addition to applying Heartbleed-TG5986 patch, ADTRAN recommends the following:
        - Replace private keys and certificates.
            - If you are using the default pre-installed self-signed certificate on the vWLAN:
                - Install the RegenerateCerts-TG6350 patch to automatically replace private keys and certificates. This patch is available here: ADTRAN vWLAN Software Downloads
            - 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
- NetVanta 1531 (ver. R11.1.0) – AOS firmware version R11.1.2 addresses the vulnerability and is now released. The firmware can be downloaded from the ADTRAN support web site.
- ADTRAN-Polycom IP Phones – Basic suggestions include (1) Placing the ADTRAN-Polycom product behind a firewall whenever possible, such that outsiders do not have access to ports used by OpenSSL on the device (usually only HTTPS, but sometimes other protocols that use TLS such as secure LDAP or secure SIP are involved)., (2) Turn off any services that use OpenSSL (if relevant) if at all possible. When new fixes become available, new certificates can be issued for your system, thus occluding any knowledge an attacker might have gained with regards to your old encryption certificates or keys. (3) Consider use of an unaffected software version based on your phone model. (4) Set the http.enabled flag to = 0 (zero). This disables web access of all kinds, and blocks known heartbeat vectors into the system

Software Versions and Fixes:

ADTRAN recommends upgrading to a release equal to or later than the release in the "Recommended Release" column of the following table:

Product	Recommended Release
vWLAN version 2.4	Heartbleed-TG5986 and RegenerateCerts-TG6350 Patch for 2.4
NetVanta 1531 version R11.1.0	R11.1.2
ADTRAN Soundpoint series IP phones (321/335/550/650) (UCS version 4.1.0.84959rts42 to UCS 4.1.6.4835rts50 only)	TBD
ADTRAN VVX series IP phones (300/310/400/410/500/600) (UCS version 4.1.3.7864rts21G to UCS 5.0.1.7396rts56 Q only)	TBD

Obtaining Fixed Software:
Software that addresses this vulnerability 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	2014-04-10	Initial release	-
B	2014-04-16	Revision B	Added Carrier Network (CN) Division products to Security Advisory notice, updated status of vWLAN software patch, updated status of Soundpoint IP and VVX phones
C	2014-04-17	Revision C	Added Total Access 1500 and 4303. Removed AOE from the list of affected products.
D	2014-04-18	Revision D	Added Total Access EMS, OPTI-6100, MX410, MX412 and MX28xx series to the list of unaffected products. Added release date for AOS R11.1.2 to address NetVanta 1531. Updated ADTRAN-Polycom IP phone workarounds.
E	2014-05-01	Revision E	Added OPTI-3 to list of products not affected. AOS firmware R11.1.2 is now officially released. Added further recommendations under temp workarounds for Bluesocket vWLAN 2.4 including replacing private keys, certs, changing passwords, PSKs and shared secrets.