ID: ADTSA-14-003	**Padding Oracle On Downgraded Legacy Encryption (POODLE) Vulnerability**	**Revision: A**

Publication Date: 2014-10-22

Summary: A vulnerability was found in the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher-block chaining (CBC) mode. This flaw allows a man-in-the-middle (MITM) attacker to decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

Solution: The only solution to fully mitigate POODLE is to disable SSL 3.0. When supported in both the client and server, TLS_FALLBACK_SCSV helps prevent protocol downgrade attacks.

Description:
SSL 3.0 is a legacy protocol used to secure communications. Recently, it was discovered that the process in which blocks of data are encrypted using CBC with SSL 3.0 can be attacked. These blocks of encrypted data can be decrypted by an attacker byte by byte if an application can be forced to replay the data over newly created SSL 3.0 connections.

POODLE specifically takes advantage of this as well as a mechanism within Transport Layer Security (TLS) which controls SSL/TLS version negotiation. A man-in-the-middle (MITM) attacker can force a responding application to continually downgrade its negotiated version of TLS until SSL 3.0 is selected and then decrypt the data to clear text.

This vulnerability is identified by CVE-2014-3566.

Affected Products:
- NetVanta 600/1000/3000/4000/5000/6000/7000 series products (all versions with a GUI)
  - HTTPS server and HTTPS client (used by Auto-Link and HTTPS packet capture exports) are affected
- Total Access 900/900e series products (all versions)
  - HTTPS server and HTTPS client (used by Auto-Link and HTTPS packet capture exports) are affected
- n-Command MSP (all versions)
  - Version 8.1.1 will disable support for SSL 3.0 and will also support TLS_FALLBACK_SCSV, date TBA
- Bluesocket vWLAN (all versions)
  - A future release will disable SSL 3.0 by default and will also support TLS_FALLBACK_SCSV, date TBA
- Bluesocket Controller (BSC) (all versions)
  - HTTPS server

Products that are still being investigated:
The following products are possibly vulnerable but still being fully investigated:

- ACI-E
- ADTRAN SoundPoint series IP phones
- ADTRAN VVX series IP phones
- AOE (Advanced Operational Environment)
- hiX products
- NetVanta 800/8000 series products
- NetVanta 2000 series products
- NetVanta Unified Communications Servers (UCS, BCS, ECS and BAS)
- OPTI-3
- OPTI-6100
- Total Access 300/400/500 series Optical Network Terminal (ONT)/Optical Network Unit (ONU)
- Total Access 1100/1200 series products
- Total Access 1400 series products

- Total Access 5000 series products
- Total Access EMS B release series

Impact:
This vulnerability is classified by industry standards as “Medium” impact with CVSS Impact Subscore 2.9 and “medium” on complexity, which means it takes moderate skill to perform. This flaw allows attackers to possibly obtain sensitive information in HTTPS sessions such as passwords, secure cookies, or other authentication tokens. These can then be used to gain unauthorized access into the same units and applications. The POODLE attack can be used against any system or application that supports SSL 3.0 with CBC encryption.

Recommendations:
Disable SSL 3.0 support in web browsers before connecting to the GUI of affected products.

Advisory Revisions and Status:

Revision	Date	Revision Description
A	2014-10-22	Initial release