ID: ADTSA-BCI1002 **Bash Code Injection Vulnerability** **Revision: D**

Publication Date: 2014-09-26 (Updated 2014-09-29)

Affected Products: None. See details below

Summary: A critical vulnerability has been reported in the GNU Bourne Again Shell (Bash) commonly found in unix derived operating systems. If exploited this vulnerability could allow an attacker to remotely execute shell commands. This article will document if and when any ADTRAN products are determined to be exploitable.

Solution: No solution is required, as no ADTRAN product is exploitable by this vulnerability

Description:
The GNU Bourne Again shell (Bash) is a shell and command language interpreter compatible with the Bourne shell. It was found that the fix for CVE-2014-6271 was incomplete, and Bash still allowed certain characters to be injected into other environments via specially crafted environment variables. An attacker could potentially use this flaw to override or bypass environment restrictions to execute shell commands. Certain services and applications allow remote unauthenticated attackers to provide environment variables, allowing them to exploit this issue (CVE-2014-7169). Additional related CVE's include:

CVE-2014-6277
CVE-2014-6278
CVE-2014-7186
CVE-2014-7187

This vulnerability is occasionally referred to as "Shellshock" and/or "Bashdoor".

Affected Products:
ADTRAN has completed its research and determined that no ADTRAN is exploitable by this vulnerability.

Impact
This vulnerability is classified by industry standards as "High" impact with CVSS Impact Subscore 10 and "Low" on complexity, which means it takes little skill to perform. This flaw allows attackers to provide specially crafted environment variables containing arbitrary commands that can be executed on vulnerable systems. It is especially dangerous because of the prevalent use of the Bash shell and its ability to be called by an application in numerous ways.

Advisory Revisions and Status:

Revision	Date	Revision Description
A	2014-09-26	Initial release
B	2014-09-29	n-Command MSP removed from possible impacted products
C	2014-09-29	Provided additional detail on regarding the vulnerability, plus general clarifications
D	2014-10-02	Updated to reflect that ADTRAN's investigations has concluded and no ADTRAN product is exploitable by this vulnerability