ADTRAN Security Advisory

ID: ADTSA-2018003 **SegementSmack Linux Kernel Vulnerability** **Revision: A**

Publication Date: 2018-08-15 (Rev. A: 2018-08-15)

Summary: SegmentSmack Linux Kernel Vulnerability (CVE-2018-5390)

Status: All products using the Linux kernel are being investigated.

Description:
ADTRAN has recently become aware of a vulnerability named "SegmentSmack" that was found in the way the Linux kernel handles specially crafted TCP packets. A remote attacker could use this flaw to trigger time and calculation expensive calls to the tcp_collapse_ofo_queue() and tcp_prune_ofo_queue() functions by sending specially modified packets within ongoing TCP sessions. This could lead to CPU saturation and denial of service (DoS) on the system. Maintaining the DoS condition requires continuous two-way TCP sessions to a reachable open port, thus the attacks cannot be performed using spoofed IP addresses.

Affected Products:

Under investigation. Affected products and updates will be promptly added as each investigation is completed.

Product Family	Solution	Suggested Actions to Mitigate
MOSAIC Device Manager	Update system packages using 'sudo yum update'	Apply the described solution.
MOSAIC Cloud Platform (OVA appliance version only)	A patch will be provided	ADTRAN will provide necessary patch as soon as analysis is complete.
nCommand MSP	A patch will be provided	ADTRAN will provide necessary patch as soon as analysis is complete.

Impact:

The severity of this vulnerability is classified as "high" by industry standards. ADTRAN will release security updates for affected products as quickly as possible following the investigation.

Advisory Revisions and Status:

Revision	Date	Revision Description
A	2018-08-15	Initial release