AppGate SDP
Security Advisory

ID: 2018-08-0001

First published	2018-08-09
Last updated	2018-08-09

Title

TCP Stack vulnerability: SegmentSmack

Summary

The flaw relates to the way the Linux kernel handles some specially crafted TCP packets. These packets, when sent within an existing TCP session can force Linux to make very expensive system calls for every incoming packet which can lead to a very high CPU utilization and eventually denial of service.

For AppGate SDP systems configured in line with our hardening recommendations the external entry points into Gateways and Controllers (port 443) are protected by Single-Packet Authorization, so are not vulnerable for unauthorized users.

The only potential points of vulnerability is the Management Interface (444), SSH console (22) and Multi-Controller Sync (5432) interfaces.

Note that this vulnerability applies to all linux kernel versions 4.9+. For more information: https://nvd.nist.gov/vuln/detail/CVE-2018-5390

Severity

Low

Products Affected

AppGate SDP appliance versions before 4.1.2 are affected.

AppGate Classic is not affected.

Suggested Action

Upgrade AppGate SDP appliances to version 4.1.2 or later.

Workaround and Mitigations

Restrict Management Interface (port 444), SSH (port 22) and Multi-Controller sync (port 5432) Access to trusted networks. Use Single-Packet Authorization for Client Interface.