

AppGate SDP Security Advisory

ID: 2018-12-0001

First published 2018-12-03
Last updated 2018-12-03

Title

Controller Impersonation during Appliance Communication.

Summary

A malicious user with access to peer interface (default: port 444) and a specially crafted certificate can impersonate the Controller and send commands to other appliances in the Collective.

Details will not be published for security reasons.

Severity

Low (CVSS 3.3)

Products Affected

AppGate SDP Appliances versions before 4.1.7.

Suggested Action

Upgrade AppGate SDP Appliances to 4.17 or later.

Workaround and Mitigations

The applicability of an attack is very low since it requires peer interface access (default: port 444) and a specially crafted certificate. This would have required prior administrative access to the production systems. Access to the peer interface must be limited to AppGate SDP admins and other appliances in the Collective in line with the best practice guide.