

AppGate SDP Security Advisory

ID: 2020-04-0002

First published 2020-05-01
Last updated 2020-05-01

Title

Remote Code Execution on Management Interface

Summary

A malicious authenticated user could use specific AppGate SDP Controller APIs to execute arbitrary code.

Severity

High (CVSS 7.5)

Products Affected

AppGate SDP Controller versions 4.1.0 through 5.0.3, 5.1.0 and 5.1.1 are affected.

Suggested Action

Upgrade AppGate SDP Controllers to version 5.0.4 or to versions 5.1.2 or later.

Workaround and Mitigations

The likelihood of an attack is very low since it requires access to the peer interface (default port: 444) or admin interface (default port: 8443) by an authenticated user, using specially crafted data. Access to the peer interface and admin interface should be limited to AppGate SDP admins and other appliances in the Collective in line with the best practice security guide.