Appgate SDP Security Advisory

ID: 2021-04-0001

First published	2021-04-15
Last updated	2021-04-23

Title

Information Disclosure from Appgate SDP Controllers

Summary

A vulnerability exists in the SAML identity provider interface of the Controller appliance, that could allow unauthorized disclosure of information from the Controller.

While the vulnerability opens up a new attack vector, as of now neither the external penetration testers nor Appgate R&D have managed to disclose any sensitive/valuable information.

Severity

High (CVSS 8.5)

Products Affected

Appgate SDP Controllers (with a SAML IdP); versions before 5.3.3 (except 5.2.4) are affected.

Suggested Action

Upgrade Appgate SDP Controllers to version 5.2.4 or 5.3.3 and above.

For Customers with v5.1 Controllers that cannot be upgraded to v5.2 or v5.3 in the near term, Appgate is providing an appliance customization to patch the vulnerability.

Workaround and Mitigations

The attack only applicable to Controllers with a SAML IdP configured.

Limiting access to the Controller's administration interface and the use of SPA to prevent unauthorized access to the Controller's Client interface will prevent this type of attack.

v5.3 Controllers require SPA be used at all times, customers with earlier version of Controllers are advised to enable SPA as soon as possible. The Client Profile Links (which contains unique SPA keys) should be kept confidential according to best practices.