

Appgate SDP Security Advisory

ID: 2020-11-0001

First published 2020-11-30
Last updated 2020-12-07

Title

Default Time-Based OTP Provider Bypass

Summary

An attacker with compromised credentials can bypass Default Time-Based OTP Provider challenges using a crafted request pattern.

Severity

Medium (CVSS 6.8)

Products Affected

Appgate SDP Controller versions before 5.3.1 are affected.

Suggested Action

Upgrade Appgate SDP Controller to version 5.3.1 and above.

Workaround and Mitigations

Only "Default Time-Based OTP Provider" MFA Provider is vulnerable. Appgate recommends all customers using "Default Time-Based OTP Provider" to upgrade to version 5.3.1 as soon as possible, or if staying with an earlier version switch to another MFA provider.

Recognition

Thanks to the following individuals for discovering and responsibly disclosing this vulnerability to Appgate:

- Eugene Lim (<https://www.linkedin.com/in/limzhiweieugene/>)
- Hui Yi Loke (<https://www.linkedin.com/in/angelystor/>)
- Max Chee (<https://www.linkedin.com/in/max-chee/>)