

# AppGate SDP Security Advisory

ID: 2018-03-0001

First published 2018-03-12  
Last updated 2018-07-12

## Title

Authentication bypass by impersonation due to incorrect processing of SAML XML token.

## Summary

A SAML-authenticated user could impersonate another user under certain configurations, by modifying the SAML token to bypass first factor authentication for the spoofed user. Under these conditions, an attacker could obtain some or all of the network entitlements corresponding to the impersonated user.

For additional details on the underlying SAML/XML parsing vulnerability, see <https://www.kb.cert.org/vuls/id/475445>

## Severity

Low

## Products Affected

AppGate SDP Controller versions before 3.3.3 are affected.

AppGate Classic server is not affected.

## Suggested Action

Upgrade AppGate SDP appliances to version 3.3.3 and above.

## Workaround and Mitigations

Attackers, who must be authenticated users, can only bypass the first factor of authentication in certain Controller/Identity Provider configurations. A second authentication factor renders this attack vector useless.