The application, when utilizing PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.

Overview

Finding ID	Version	Rule ID	IA Controls	Severity
V-222550	APSC-DV-001810	SV-222550r879612_rule		High

Description

Without path validation, an informed trust decision by the relying party cannot be made when presented with any certificate not already explicitly trusted. A trust anchor is an authoritative entity represented via a public key and associated data. It is used in the context of public key infrastructures, X.509 digital certificates, and DNSSEC. When there is a chain of trust, usually the top entity to be trusted becomes the trust anchor; it can be, for example, a Certification Authority (CA). A certification path starts with the subject certificate and proceeds through a number of intermediate certificates up to a trusted root certificate, typically issued by a trusted CA. This requirement verifies that a certification path to an accepted trust anchor is used for certificate validation and that the path includes status information. Path validation is necessary for a relying party to make an informed trust decision when presented with any certificate not already explicitly trusted. Status information for certification paths includes certificate revocation lists or online certificate status protocol responses. Validation of the certificate status information is out of scope for this requirement.

STIG	Date
Application Security and Development Security Technical Implementation Guide	2023-06-08

Details

Check Text (C-24220r493558_chk)

Review the application documentation, the application architecture and interview the application administrator to identify the method employed by the application for validating certificates.

Review the method to determine if a certification path that includes status information is constructed when certificate validation occurs.

Some applications may utilize underlying OS certificate validation and certificate path building capabilities while others may build the capability into the application itself.

The certification path will include the intermediary certificate CAs along with a status of the CA server's signing certificate and will end at the trusted root anchor.

If the application does not construct a certificate path to an accepted trust anchor, this is a finding.

Fix Text (F-24209r493559_fix)

Design the application to construct a certification path to an accepted trust anchor when using PKI-based authentication.