Service-Oriented Applications handling non-releasable data must authenticate endpoint devices via mutual SSL/TLS.

Overview

Finding ID	Version	Rule ID	IA Controls	Severity
V-222534	APSC-DV-001660	SV-222534r879768_rule		Medium

Description

Without identifying devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity. One way SSL/TLS authentication is the typical form of authentication done between a web browser client and a web server. The client requests the server certificate to validate the server's identity and establish a secure connection. When SSL/TLS mutual authentication is used, the server is configured to request the client's certificate as well so the server can also identify the client. This form of authentication is normally chosen for system to system communications that leverage HTTP as the transport. It should be noted that SSL is being deprecated and replaced with TLS. For distributed architectures (e.g., service-oriented architectures), the decisions regarding the validation of identification claims may be made by services separate from the services acting on those decisions. In such situations, it is necessary to provide the identification decisions (as opposed to the actual identifiers) to the services that need to act on those decisions. This requirement applies to applications that connect either locally, remotely, or through a network to an endpoint device (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs). Gateways and SOA applications are examples of where this requirement would apply.

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

Details

Check Text (C-24204r493510_chk)

Review application documentation and interview application administrator.

Identify application data elements and determine if the application is handling/processing non-releasable data.

Review the application architecture and design documents.

Identify endpoint devices that interact with the application. These can be SOA gateways, VOIP phones, or other devices that are used to connect to and exchange data with the application.

If the design documentation specifies it, this could also include remote client workstations. However, this requirement is usually reserved for system-oriented endpoints rather than client workstations.

In order for two way SSL/TLS mutual authentication to work properly, the server must be configured to request client certificates.

Access the applications management console and navigate to the SSL/TLS management utility or web page that is used to configure two-way mutual authentication.

Verify endpoints are configured for client authentication (mutual authentication).

Some application architectures configure their settings in text/xml formatted files; in that case, have the application administrator identify the configuration files used by the application (e.g., web.xml stored in WEB-INF/ sub directory of the application root folder).

Open the web.xml file using a text editor and verify the application deployment descriptor for the application and the resource requiring protection under the "login-config" element is set to CLIENT-CERT.

If SSL/TLS mutual authentication is required due to the application processing non-releasable data and SSL/TLS mutual authentication not being utilized, this is a finding.

Fix Text (F-24193r493511_fix)

Configure the application to utilize mutual authentication when the application is processing non-releasable data.