The application must not expose session IDs.

Overview

Finding ID	Version	Rule ID	IA Controls	Severity
V-222577	APSC-DV-002230	SV-222577r879636_rule		High

Description

Authenticity protection provides protection against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions. Application communication sessions are protected utilizing transport encryption protocols, such as SSL or TLS. SSL/TLS provides web applications with a means to be able to authenticate user sessions and encrypt application traffic. Session authentication can be single (one-way) or mutual (two-way) in nature. Single authentication authenticates the server for the client, whereas mutual authentication provides a means for both the client and the server to authenticate each other. This requirement applies to applications that utilize communications sessions. This includes, but is not limited to, web-based applications and Service-Oriented Architectures (SOA). This requirement addresses communications protection at the application session, versus the network packet, and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Depending on the required degree of confidentiality and integrity, web services/SOA will require the use of SSL/TLS mutual authentication (two-way/bidirectional).

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

Details

Check Text (C-24247r493639_chk)

Review the application documentation and configuration.

Interview the application administrator and obtain implementation documentation identifying system architecture.

Identify the application communication paths. This includes system to system communication and client to server communication that transmit session identifiers over the network.

Have the application administrator identify the methods and mechanisms used to protect the application session ID traffic. Acceptable methods include SSL/TLS both one-way and two-way and VPN tunnel.

The protections must be implemented on a point-to-point basis based upon the architecture of the application.

For example; a web application hosting static data will provide SSL/TLS encryption from web client to the web server. More complex designs may encrypt from application server to application server (if applicable) and application server to database as well.

If the session IDs are unencrypted across network segments, this is a finding.

Fix Text (F-24236r493640_fix)

Configure the application to protect session IDs from interception or from manipulation.