The application must implement cryptographic mechanisms to protect the integrity of remote access sessions.

Overview

Finding ID	Version	Rule ID	IA Controls	Severity
V-222397	APSC-DV-000170	SV-222397r879520_rule		Medium

Description
Without integrity protection mechanisms, unauthorized individuals may gain access to sensitive information via a remote access session. Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless. Encryption provides a means to secure the remote connection to prevent unauthorized access to the data traversing the remote access connection. Without integrity protection mechanisms, unauthorized individuals may be able to insert inauthentic content into a remote session. The encryption strength of mechanism is selected based on the security categorization of the information.

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

Details

Check Text (C-24067r493099_chk)

Review the application documentation and interview the system administrator.

Identify the application encryption capabilities and methods for implementing encryption protection.

For web based applications; open the web browser and access the website URL. Use the browser and determine if the session is protected via TLS. A secure connection is usually indicated in the upper left hand corner of the URL by a padlock icon. Click on the padlock icon and examine the connection information. Determine if TLS encryption is used to secure the session.

For non-web based applications, determine the TCP/IP port, protocol and method used for establishing client connections to the remote server. Review application configuration settings to ensure encryption is specified and via TLS.

If the connection is not secured with TLS, this is a finding.

Fix Text (F-24056r493100_fix)

Design and configure applications to use TLS encryption to protect the integrity of remote access sessions.

© 2018 Network Frontiers LLC

All right reserved.

Stay connected with UCF

QUICK LINKS

Home

Company

Products

Partners

Peer Review

Contact

Support

Legal

CONTACT

10161 Park Run Drive, Suite 150
Las Vegas, Nevada 89145

PHONE 702.776.9898
FAX 866.924.3791
info@unifiedcompliance.com

Common Controls Hub

Scope, Define, and Maintain Regulatory Demands Online in Minutes.

READ MORE