The application must protect the confidentiality and integrity of transmitted information.

Overview

Finding ID	Version	Rule ID	IA Controls	Severity
V-222596	APSC-DV-002440	SV-222596r879810_rule		High

Description

Without protection of the transmitted information, confidentiality and integrity may be compromised since unprotected communications can be intercepted and either read or altered. This requirement applies to those applications that transmit data, or allow access to data non-locally. Application and data owners have a responsibility for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process. Application and data owners need to identify the data that requires cryptographic protection. If no data protection requirements are defined as to what specific data must be encrypted and what data is non-sensitive and doesn't require encryption, all data must be encrypted. When transmitting data, applications need to leverage transmission protection mechanisms, such as TLS, SSL VPNs, or IPSEC. Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

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

Details

Check Text (C-24266r493696_chk)

Review the application documentation and interview the application administrator.

Identify application clients, servers and associated network connections including application networking ports.

Identify the types of data processed by the application and review any documented data protection requirements.

Identify the application communication protocols.

Review application documents for instructions or guidance on configuring application encryption settings.

Verify the application is configured to enable encryption protections for data in accordance with the data protection requirements. If no data protection requirements exist, ensure all application data is encrypted.

If the application does not utilize TLS, IPsec or other approved encryption mechanism to protect the confidentiality and integrity of transmitted information, this is a finding.

Fix Text (F-24255r493697_fix)

Configure all of the application systems to require TLS encryption in accordance with data protection requirements.

© 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