

The application must maintain the confidentiality and integrity of information during reception.

Overview

Finding ID	Version	Rule ID	IA Controls	Severity
V-222599	APSC-DV-002470	SV-222599r879813_rule		Medium

Description

Data is subject to manipulation and other integrity related attacks whenever that data is transferred across a network. To protect data integrity during transmission, the application must implement mechanisms to ensure the integrity of all transmitted information. All transmitted information means that the protections are not restricted to just the data itself. Protection mechanisms must be extended to include data labels, security parameters or metadata if data protection requirements specify. Modern web application data transfer methods can be complex and are not necessarily just point-to-point in nature. Service-Oriented Architecture (SOA) and RESTFUL web services allow for XML-based application data to be transmitted in a manner similar to network traffic wherein the application data is transmitted along multiple servers' hops. In such cases, point-to-point protection methods like TLS or SSL may not be the best choice for ensuring data integrity and alternative data integrity protection methods like XML Integrity Signature protections where the XML payload itself is signed may be required as part of the application design. Overall application design and architecture must always be taken into account when establishing data integrity protection mechanisms. Custom-developed solutions that provide a file transfer capability should implement data integrity checks for incoming and outgoing files. Transmitted information requires mechanisms to ensure the data integrity (e.g., digital signatures, SSL, TLS, or cryptographic hashing).

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

Details

Check Text (C-24269r493705_chk)

Review the application documentation and interview the application administrator.

Identify web servers and associated network connections.

Access the application with a web browser.

Verify the web browser goes secure automatically by automatically redirecting the browser to a secure port running TLS encryption, or ensure the port used by the application uses TLS encryption by default.

For tiered applications, (web server, application server, database server) ensure the communication channels between the tiers is also encrypted.


If the application does not utilize TLS to protect the confidentiality and integrity of transmitted information, this is a finding.

Fix Text (F-24258r493706_fix)

Configure all of the application systems to require TLS encryption.



© 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