The application must implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by alternative physical safeguards, such as, at a minimum, a Protected Distribution System (PDS).

Overview

Finding ID	Version	Rule ID	IA Controls	Severity
V-222597	APSC-DV-002450	SV-222597r879811_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-36250r602313_chk)

Review the application documentation, the application architecture designs and interview the application administrator.

Ask the application admin to identify the network path taken by the application data and demonstrate the application support integrity mechanisms for transmission of both incoming and outgoing files and any transmitted data.

For example, hashing/digital signature and cyclic redundancy checks (CRCs) can be used to confirm integrity on data streams and transmitted files.

Use of TLS can be used to assure integrity in point-to-point communication sessions.

When the application uses messaging or web services or other technologies where the data can traverse multiple hops, the individual message or packet must be encrypted to protect the integrity of the message.

If the application is not configured to provide cryptographic protections to application data while it is transmitted unless protected by alternative safety measures like a PDS, this is a finding.

Fix Text (F-36214r602314_fix)

Configure the application to use cryptographic protections to prevent unauthorized disclosure of application data based upon the application architecture.