Applications used for non-local maintenance sessions must implement cryptographic mechanisms to protect the integrity of non-local maintenance and diagnostic communications.

Overview

Finding ID	Version	Rule ID	IA Controls	Severity
V-222562	APSC-DV-001940	SV-222562r879784_rule		Medium

Description
Privileged access contains control and configuration information which is particularly sensitive, so additional protections are necessary. This is maintained by using cryptographic mechanisms to protect integrity. Non-local maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. This requirement applies to hardware/software diagnostic test equipment or tools. This requirement does not cover hardware/software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch). The application can meet this requirement through leveraging a cryptographic module.

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

Details

Check Text (C-24232r493594_chk)

Review the application documentation and interview the application administrator to identify application maintenance functions.

If the application does not provide non-local maintenance and diagnostic capability, this requirement is not applicable.

Identify the maintenance functions/capabilities that are provided by the application and performed by an individual which can be performed remotely.

For example, the application may provide the ability to clean up a folder of temporary files, add users, remove users, restart processes, backup certain files, manage logs, or execute diagnostic sessions.

Access the application in the appropriate role needed to execute maintenance tasks. Observe the manner in which the application is connecting and ensure the session is being encrypted.

For example, observe the browser to ensure the session is being encrypted with TLS/SSL.

If the application provides remote access to maintenance functions and capabilities and the remote access methods are not encrypted, this is a finding.

Fix Text (F-24221r493595_fix)

Configure the application to encrypt remote application maintenance sessions.

CONTACT

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

PHONE 702.776.9898
FAX 866.924.3791
info@unifiedcompliance.com