The application must execute without excessive account permissions.

Overview

Finding ID	Version	Rule ID	IA Controls	Severity
V-222430	APSC-DV-000510	SV-222430r879719_rule		High

Description

Applications are often designed to utilize a user account. The account represents a means to control application permissions and access to OS resources, application resources or both. When the application is designed and installed, care must be taken not to assign excessive permissions to the user account that is used by the application. An application operating with unnecessary privileges can potentially give an attacker access to the underlying operating system or if the privileges required for application execution are at a higher level than the privileges assigned to organizational users invoking such applications/programs, those users are indirectly provided with greater privileges than assigned by organizations. Applications must be designed and configured to operate with only those permissions that are required for proper operation.

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

Details

Check Text (C-24100r493198_chk)

Review the system documentation or interview the application representative and identify if the application utilizes an account in order to operate.

Determine the OS user groups in which each application account is a member. List the user rights assigned to these users and groups using relevant OS commands and evaluate whether any of them provide admin rights or if they are unnecessary or excessive.

If the application connects to a database, open an admin console to the database and view the database users, their roles and group rights.

Locate the application user account used to access the database and examine the accounts privileges. This includes group privileges.

If the application user account has excessive OS privileges such as being in the admin group, database privileges such as being in the DBA role, has the ability to create, drop, alter the database (not application database tables), or if the application user account has other excessive or undefined system privileges, this is a finding.

Fix Text (F-24089r493199_fix)

Configure the application accounts with minimalist privileges. Do not allow the application to operate with admin credentials.

UCF

© 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

UCF Common Controls Hub

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

READ MORE