HotFix KB496276 - Vulnerability in MiCCSDK could allow an authenticated user access to sensitive information in Site-Based Security environments

PROBLEM

The hotfix addresses a vulnerability in the MiContact Center Business Software Development Kit (SDK) that could allow an authenticated user access to sensitive information. The exposure is constrained to systems configured for site based security.

RESOLUTION

This Hotfix is to be installed onto **MiContact Center Business version 9.0.1.0**.

1. Ensure that KB447353 is installed.
2. Ensure that KB466294 is installed.
3. Ensure that KB470763 is installed.
4. Ensure that KB470782 is installed.
5. Ensure that KB471979 is installed.
6. Go to https://www.mitel.com/
7. Click the **Login** button.
8. Click the **Sign in** button under **MiAccess**.
9. On the left, select the **Software Download Center**.
10. Expand the tree to **MiContact Center Business** and then down to **MiContact Center Business 9.0.1.0** and **HotFixes**.
11. Download the **KB496276** HotFix to the MiContact Center server.
12. Double-click the **KB496276** and follow the on-screen prompts.
13. Wait for the repackager and auto-updates to complete.

NOTE: Installing this Hotfix will restart the MiContact Center services. To avoid service interruption install this patch after hours or during a scheduled maintenance window.

APPLIES TO

MiCC 9.0.1.0

Keywords: Hotfix 496276 KB496276 site-based security multi-tenant miccsdk

Last Modified By: montpetit.a, Friday, February 14, 2020
http://micc.mitel.com/kb/KnowledgebaseArticle52651.aspx

Friday, August 12, 2022