Sensitive Information Leakage

Advisory Original Release Date: March 2, 2005
Last Revised: August 11, 2005
Number: ASA-2005-041
Risk Level: Medium
Advisory Version: 2.0

Advisory Status: Interim

Overview:

A sensitive information leakage vulnerability exists in certain Avaya software applications and system products. In this context, sensitive information may include applications settings and/or user credentials. Affected Avaya applications store this sensitive information in the Windows registry or application files. The information is stored in manner that is weakly obfuscated or, in some cases, clear text. If a perpetrator were able to gain access to this information, they could access the application and related services impersonating the targeted user whose credentials were compromised.

In order to access this sensitive information, a perpetrator would need local or remote access to the Windows registry or file system of the targeted user. Under the Windows Operating System, all local users have access to the Windows registry and file system where this sensitive information may be stored. Only users with Administrative group privileges can remotely access the Windows registry (by default, on Windows NT 4.0 and later systems).

For certain applications, risk of compromise can be reduced by not selecting the “Remember Password” or “Save Password” option within the application.

The Common Vulnerability and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0506 to this issue.

August 2005 Update:

Avaya IPSoftphone 5.2 Service Pack 1 (SP1) has been released which includes a fix to address the above vulnerability in IPSoftphone. The fix in SP1 implements a secure algorithm to encrypt user credentials in the Windows registry. Additionally, uncheck marking the “Remember password” option in IPSoftphone now clears the encrypted information from the Windows registry. Please see the recommendations sections for more information.

Affected Software-Only Products

Product	Affected S/W Version	Comments and Recommended Actions	Risk Level
Avaya IP Softphone	All Versions	Avaya IPSoftphone 5.2 SP1 has been released to address this vulnerability. All users should apply	Low

		SP1 (see below for more information). User passwords (i.e. PINs) are only stored if the “Remember password for next login session” option is selected. Saved passwords are weakly obfuscated. Additional application data may be stored in the clear. In Release 5.2 Administrators can disable the “Remember password” option for users.	
Avaya IP Agent	All Versions	User passwords (i.e. PINs) are only stored if the “Remember password for next login session” option is selected. Saved passwords are weakly obfuscated. Additional application data may be stored in the clear. An update is being considered for a future version.	Low
Avaya IP Softconsole	All Versions	User passwords (i.e. PIN) are only stored if the “Remember password for next login session” option is selected. Saved passwords are weakly obfuscated. Additional application data may be stored in the clear. An update is being considered for a future version.	Low
Avaya IP Office Phone Manager	All Versions	Saved passwords are weakly obfuscated. Additional application data may be stored in the clear. An update is being considered for a future version.	Medium
Avaya IP Office VoiceMail Pro	All Versions	Saved passwords are weakly obfuscated. Additional application data may be stored in the clear. An update is being considered for a future version.	Medium
Avaya IP Office TAPI	All Versions	Saved passwords are weakly obfuscated. Additional application data may be stored in the clear. An update is being considered for a	Medium

		future version.	
Avaya CMS Supervisor	All Versions	User credentials are only stored if the user creates a CMS Supervisor scheduled task such as saving and printing a report. Saved user credentials are weakly obfuscated. An update is being considered for a future version.	Low
Avaya Interactive Response	All Versions	This product can optionally be configured to access a database. If access to the database is controlled by an ID and password, those credentials are stored in clear text. This issue will be addressed in Release 2.0	Low

Avaya System Products:

Avaya Conversant/ Interactive Voice Response	All Versions	This product can optionally be configured to access a database. If access to the database is controlled by an ID and password, those credentials are stored in clear text. An update is being considered for a future version.	Low

Recommended Actions for the IP Softphone

Avaya recommends all users apply the Avaya IPSoftphone 5.2 Service Pack 1. The Avaya IPSoftphone 5.2 Service Pack 1 is available for download from:

http://support.avaya.com/japple/css/japple?temp.documentID=251593&temp.productID=107767&temp.releaseID=227980&temp.bucketID=108025&PAGE=Document

A list of fixes in Service Pack 1 and instructions on how to apply the Service Pack are available in the Product Correction Notice at:

http://support.avaya.com/japple/css/japple?temp.documentID=251593&temp.productID=107767&temp.releaseID=227980&temp.bucketID=108025&PAGE=Document

Recommended Actions for IP Agent and IP Softconsole:

Avaya recommends against selecting the “Remember password” option in affected applications. Note that unselecting the “Remember password” option discontinues use of the registry information (i.e. saved password) to log into the application but does not clear the registry settings.

In order to clear the registry settings, users must attempt to login using a known bad password while the “Remember password” option is selected. This overwrites the registry entries. Once this action has been performed the “Remember password” option should be deselected.

Recommended Actions for all applications:

Congruent with generally accepted security practices, Avaya recommends that local user and Windows registry access is restricted on affected systems until an update can be applied. For more information about restricting remote access to the Windows registry see Microsoft Knowledge Base article Q153183:

http://support.microsoft.com/kb/153183

Additional Information: Additional information may also be available via the Avaya support website (http://support.avaya.com) and through your Avaya account representative. Please contact your Avaya product support representative, or dial 1-866-GO-AVAYA, with any questions.

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED "AS IS". AVAYA INC., ON BEHALF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS “AVAYA”), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS’ SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.

Revision History:

V 1.0 - March 2, 2005 - Initial statement issued.
V 2.0 - August 11, 2005 - IP Softphone SP1 information added.

Send information regarding any discovered security problems with Avaya products to either the contact noted in the product's documentation or securityalerts@avaya.com.