

VPNRemote Credentials Disclosure

Advisory Original Release Date: November 23, 2005

Last Revised: November 23, 2005

Number: ASA-2005-230

Risk Level: Low

Advisory Version: 1.0

Advisory Status: Interim

Overview:

Avaya VPN (Virtual Private Networking) software applications and system products are security appliances designed to provide users secure remote access over IP networks.

While performing vulnerability research, Adrian Pastor (NTA Monitor) discovered a local password disclosure vulnerability in the Avaya VPNRemote software. Certain Avaya Virtual Private Networking (VPN) software applications store user credentials (username and password) in clear-text in process memory. This vulnerability could allow a local attacker, with access to process memory, to obtain the VPN user's username and password. The Common Vulnerability and Exposures project (cve.mitre.org) has assigned the name [CVE-2005-2762](https://cve.mitre.org/cve/2005/2762) to this issue.

Mitigating Factors:

In order to access these credentials, an attacker would need local access to the VPN software process memory and the VPN software would need to be running with an established and authenticated VPN session.

Affected Software-Only Products

Product	Affected S/W Version	Comments and Recommended Actions	Risk Level
Avaya VPNRemote	All Versions prior to 4.2.33.	Avaya VPNRemote version 4.2.33 has been released to address this vulnerability. All users should apply version 4.2.33 (or later) to address this vulnerability (see below for more information).	Low
Avaya VPNRemote for Pocket PC (PPC)	All Versions	A patch is being considered for a future release.	Low

Recommended Actions for the VPNRemote

Avaya recommends all users apply Avaya VPNRemote version 4.2.33 (or later). Avaya VPNRemote version 4.2.33 is available for download from:

ftp://vpnet:vpn365@ftp.avaya.com/incoming/guests/vpnet/vpnremote4.2/Avaya_VPNremote_for_Windows_v4.2.33.exe

OR by performing the following steps at a Windows command prompt:

- 1.) *ftp ftp.avaya.com*
- 2.) When prompted for the user, type *vpnet*
- 3.) When prompted for the password, type *vpn365*
- 4.) To Change Directories, type *cd vpnremote4.2*
- 5.) To download the new VPNRemote version, type *get Avaya_VPNremote_for_Windows_v4.2.33.exe*
- 6.) To end the ftp session, type *bye*

To obtain the password for the downloaded file, please email vpnsupport@avaya.com or call the Avaya Support Center at 800-237-0016 X 73113.

Acknowledgements:

Avaya thanks and credits Adrian Pastor and NTA Monitor for bringing this issue to our attention as well as working with Avaya to help protect customers.

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 1-800-242-2121, 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 - November 23, 2005 - Initial statement issued.

securityalerts@avaya.com.

© 2005 Avaya Inc. All Rights Reserved. All trademarks identified by the ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.