Windows Security Updates for November 2005 - (MS05-053)

Advisory Original Release Date: November 8, 2005
Last Revised: November 8, 2005
Number: ASA-2005-228
Risk Level: Low
Advisory Version: 1.0

Advisory Status: Final

Overview: Microsoft issued a security bulletin summary for November 2005 which contained one security advisory: MS05-053. This advisory describes vulnerabilities in the Microsoft Operating System. A description of the vulnerability can be found at:

http://www.microsoft.com/technet/security/bulletin/ms05-nov.mspx

Certain Avaya products utilize Microsoft Operating Systems and may be affected by this vulnerability.

Avaya Software-Only Products

Avaya software-only products operate on general-purpose Operating Systems. Occasionally vulnerabilities may be discovered in the underlying Operating System or applications which come with the Operating System. These vulnerabilities often do not impact the software-only product directly but may threaten the integrity of the underlying platform.

In the case of this advisory Avaya software-only products are not affected by the vulnerabilities directly but the underlying Microsoft platform may be. For affected Microsoft Operating Systems, Microsoft recommends installing patches. Detailed instructions from patching the Operating System are given by Microsoft at the following link:

http://www.microsoft.com/technet/security/Bulletin/MS05-053.mspx

The following Avaya software-only products run on Microsoft Operating Systems and may have been installed on a vulnerable Microsoft Operating System. Customers should determine on which Microsoft Operating System the product was installed and then follow Microsoft's guidance for applying patches:

Software-Only Products

Product	Software Version
Avaya Agent Access	All Versions
Avaya Basic Call Management System Reporting Desktop – server	All Versions
Avaya Basic Call Management System Reporting Desktop – client	All Versions
Avaya CMS Supervisor	All Versions

Avaya Computer Telephony	All Versions
Avaya CVLAN Client	All Versions
Avaya Enterprise Manager	All Versions
Avaya Integrated Management	All Versions
Avaya Interaction Center	All Versions
Avaya Interaction Center – Voice Quick Start	All Versions
Avaya IP Agent	All Versions
Avaya IP Softphone	All Versions
Avaya Modular Messaging	All Versions
Avaya Network Reporting	All Versions
Avaya OctelAccess® Server	All Versions
Avaya OctelDesigner™	All Versions
Avaya Operational Analyst	All Versions
Avaya Outbound Contact Management	All Versions
Avaya Speech Access	All Versions
Avaya Unified Communication Center	All Versions
Avaya Unified Messenger ®	All Versions
Avaya Visual Messenger ™	All Versions
Avaya Visual Vector Client	All Versions
Avaya VPNmanager™ Console	All Versions
Avaya Web Messenger	All Versions

Avaya System Products

Avaya system products include an Operating System with the product when it is delivered. The system products described below are delivered with a Microsoft Operating System. Actions to be taken with these products are also described below.

Product	**Affected S/W Version**	**Recommended Actions**
Unified Communications Center (UCC) - S3400	All Versions	Follow Microsoft's recommendation for installing the Operating System patch: MS05-053 The Unified Communications Center product is deployed with the Microsoft Windows 2000 Operating System.
Modular Messaging - Messaging Application Server (MAS)	All Versions	Follow Microsoft's recommendation for installing the Operating System patch: MS05-053 The Modular Messaging - Messaging Application Server (MAS) is deployed with the Microsoft Windows 2000

		Operating System.
S8100/DefinityOne/IP600 Media Servers	All Versions	Follow Microsoft's recommendation for installing the Operating System patch: MS05-053 These products are deployed with either the Microsoft Windows 2000 Operating System or the Microsoft Windows NT Operating System.

Recommended Actions: Avaya recommends that the Microsoft patches and/or workaround solutions are applied for the vulnerability outlined in the above system product table.

Although certain Avaya system products utilize Microsoft Operating Systems and may be affected by this vulnerability, Avaya recommends that the use of e-mail clients and Internet browsers be restricted on Avaya system products (i.e. Outlook Express and Internet Explorer). The use of browsers should be restricted to authorized users-only as well as limited to the operational-needs of the product. Unrestricted access to the Intranet or Internet should be prohibited beyond the necessary functions of the product's web administration interface and to obtaining patches. This reduces the risk of vulnerabilities in these applications.

Further information regarding the Microsoft patches on Avaya system products is below:

MS05-053 Vulnerabilities in Graphics Rendering Engine Could Allow Code Execution (896424): A remote code execution vulnerability exists in the rendering of Windows Metafile (WMF) and Enhanced Metafile (EMF) image formats that could allow remote code execution on an affected system. Any program that renders WMF or EMF images on the affected systems could be vulnerable to this attack. Another remote code execution vulnerability exists in the rendering of Windows Metafile (WMF) image format that could allow remote code execution on an affected system. Any program that renders WMF images on the affected systems could be vulnerable to this attack. An attacker who successfully exploited these vulnerabilities could take complete control of an affected system. A denial of service vulnerability exists in the rendering of Enhanced Metafile (EMF) image format that could allow any program that renders EMF images to be vulnerable to attack. An attacker who successfully exploited this vulnerability could cause the affected programs to stop responding. Each of these vulnerabilities requires an attacker to persuade a system user to open a specially crafted file to be exploited. These vulnerabilities impact S8100/DefinityOne/IP600 Media Servers, Modular Messaging Message Application Server (MAS), and Unified Communication Center. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the names CAN-2005-2123, CAN-2005-2124, and CAN-2005-0803 to these issues.

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 1-800-241-2121, 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 8, 2005 - Initial statement issued.

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