Windows Security Updates for February 2005 - (MS05-004 - MS05-015)

Advisory Original Release Date: February 9, 2005
Last Revised: February 9, 2005
Number: ASA-2005-037
Risk Level: High
Advisory Version: 1.0

Advisory Status: Final

Overview: Microsoft issued a security bulletin summary for February 2005 which contained twelve security advisories: MS05-004, MS05-005, MS05-006, MS05-007, MS05-008, MS05-009, MS05-010, MS05-011, MS05-012, MS05-013, MS05-014 and MS05-015. These advisories describe vulnerabilities in the Microsoft Operating System or applications. A description of the vulnerabilities can be found at:

http://www.microsoft.com/security/bulletins/200502_windows.mspx

Certain Avaya products utilize Microsoft Operating Systems and may be affected by these vulnerabilities.

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 these advisories 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 links:

http://www.microsoft.com/technet/security/bulletin/MS05-004.mspx

http://www.microsoft.com/technet/security/bulletin/MS05-005.mspx

http://www.microsoft.com/technet/security/bulletin/MS05-006.mspx

http://www.microsoft.com/technet/security/bulletin/MS05-007.mspx

http://www.microsoft.com/technet/security/bulletin/MS05-008.mspx

http://www.microsoft.com/technet/security/bulletin/MS05-009.mspx

http://www.microsoft.com/technet/security/bulletin/MS05-010.mspx

http://www.microsoft.com/technet/security/bulletin/MS05-011.mspx

http://www.microsoft.com/technet/security/bulletin/MS05-012.mspx

http://www.microsoft.com/technet/security/bulletin/MS05-013.mspx

http://www.microsoft.com/technet/security/bulletin/MS05-014.mspx

http://www.microsoft.com/technet/security/bulletin/MS05-015.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 patches: MS05-004, MS05-008, MS05-011, MS05-012, MS05-013, MS05-014 and MS05-015. 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 patches: MS05-004, MS05-008, MS05-011, MS05-012, MS05-013, MS05-014 and MS05-015. 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 patches: MS05-008, MS05-011, MS05-012, MS05-013, MS05-014 and MS05-015. 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 vulnerabilities outlined in the above system product table.

Although certain Avaya system products utilize Microsoft Operating Systems and may be affected by these vulnerabilities, 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:

MS05-004 - This vulnerability impacts ASP.NET. A canonicalization vulnerability exists in ASP.NET that could allow an attacker to bypass the security of an ASP.NET Web site and gain unauthorized access. An attacker who successfully exploited this vulnerability could take a variety of actions, depending on the specific contents of the website. Avaya Modular Messaging 2.0, and later, utilizes ASP.NET for VoiceXML. However, HTTP and ASP.NET access is restricted to the localhost on the Message Application Server (MAS) and therefore exploitation of this vulnerability is restricted to local authenticated users.

MS05-005 - A vulnerability exists in Microsoft Office XP software that could allow remote code execution on an affected system. An attacker who successfully exploited this vulnerability could take complete control of the affected system. Avaya system products do not ship with Microsoft Office XP and are therefore not affected by this vulnerability.

MS05-006 - A cross-site scripting and spoofing vulnerability exists in Microsoft SharePoint and SharePoint team services. This vulnerability could allow an attacker to convince a user to run a malicious script. Avaya system products do not ship with Microsoft SharePoint or SharePoint team services and are therefore not affected by this vulnerability.

MS05-007 - An information disclosure vulnerability exists in Microsoft Windows XP's Computer Browser service. An attacker who successfully exploited this vulnerability could remotely read the user names for users who have an open connection to an available shared resource. Avaya system products do not operate on Windows XP and therefore are not affected by this vulnerability.

MS05-008 - A privilege elevation vulnerability exists in Windows because of the way that Windows handles drag-and-drop events. An attacker could exploit the vulnerability by constructing a malicious Web page. This malicious Web page could potentially allow an attacker to save a file on the user's system if a user visited a malicious Web site or viewed a malicious e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system. This vulnerability impacts S8100/DefinityOne/IP600 Media Servers, Messaging Application Server (MAS), and Unified Communication Center. However, user interaction is required to exploit this vulnerability.

MS05-009 - A remote code execution vulnerability exists in Windows Media Player, MSN Messenger, and Windows Messenger handling of PNG files. An attacker could try to exploit the vulnerability by constructing a malicious PNG that could potentially allow remote code execution if a user visited a malicious Web site or clicked a link in a malicious e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system. Avaya system products do not ship with affected versions of Windows Media Player, MSN Messenger, or Windows Messenger and are therefore not affected by this vulnerability.

MS05-010 - A remote code execution vulnerability exists in the Windows License Logging service. This vulnerability could allow an attacker who successfully

exploited this vulnerability to take complete control of the affected system. Avaya system products do not ship with the License Logging service enabled and are therefore not affected by this vulnerability.

MS05-011 - A remote code execution vulnerability exists in Windows Server Message Block (SMB). This vulnerability could allow an attacker who successfully exploited this vulnerable to take complete control of the affected system. This vulnerability impacts S8100/DefinityOne/IP600 Media Servers, Messaging Application Server (MAS), and Unified Communication Center.

MS05-012 - Two separate vulnerabilities exist in Windows COM and OLE. An attacker who successfully exploited these vulnerabilities could take complete control of an affected system. These vulnerabilities impact S8100/DefinityOne/IP600 Media Servers, Messaging Application Server (MAS), and Unified Communication Center. However, on Avaya system products, local user access or user interaction is required to exploit these vulnerabilities.

MS05-013 - A cross-domain vulnerability exists in the Microsoft Dynamic HTML (DHTML) Editing Component ActiveX control. This vulnerability could allow information disclosure or remote code execution on an affected system. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited that page. An attacker who successfully exploited this vulnerability could take complete control of an affected system. This vulnerability impacts S8100/DefinityOne/IP600 Media Servers, Messaging Application Server (MAS), and Unified Communication Center.

MS05-014 - Multiple vulnerabilities exist in Microsoft Internet Explorer. These vulnerabilities could allow remote code execution on an affected system. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited that page. An attacker who successfully exploited this vulnerability could take complete control of an affected system. These vulnerabilities impact S8100/DefinityOne/IP600 Media Servers, Messaging Application Server (MAS), and Unified Communication Center. On Avaya system products user interaction is required to exploit these vulnerabilities.

MS05-015 - A remote code execution vulnerability exists in the Hyperlink Object Library. An attacker could exploit the vulnerability by constructing a malicious hyperlink which could potentially lead to remote code execution if a user clicks a malicious link within a Web site or e-mail message. An attacker who successfully exploited this vulnerability could take complete control of the affected system. This vulnerability impacts S8100/DefinityOne/IP600 Media Servers, Messaging Application Server (MAS), and Unified Communication Center. On Avaya system products user interaction is required to exploit this vulnerability.

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 – February 9, 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.

© 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.