Windows Security Updates for October 2005 - (MS05-044-MS05-052)

Advisory Original Release Date: October 11, 2005
Last Revised: October 11, 2005
Number: ASA-2005-214
Risk Level: High
Advisory Version: 1.0

Advisory Status: Final

Overview: Microsoft issued a security bulletin summary for October 2005 which contained nine security advisories: MS05-044, MS05-045, MS05-046, MS05-047, MS05-048, MS05-048, MS05-049, MS05-050, MS05-051, and MS05-052. This advisory describes vulnerability in the Microsoft Operating System. A description of the vulnerability can be found at:

http://www.microsoft.com/technet/security/bulletin/ms05-oct.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/MS05-044.mspx

http://www.microsoft.com/technet/security/Bulletin/MS05-045.mspx

http://www.microsoft.com/technet/security/Bulletin/MS05-046.mspx

http://www.microsoft.com/technet/security/Bulletin/MS05-047.mspx

http://www.microsoft.com/technet/security/Bulletin/MS05-048.mspx

http://www.microsoft.com/technet/security/Bulletin/MS05-049.mspx

http://www.microsoft.com/technet/security/Bulletin/MS05-050.mspx

http://www.microsoft.com/technet/security/Bulletin/MS05-051.mspx

http://www.microsoft.com/technet/security/Bulletin/MS05-052.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: MS05-044, MS05-045, MS05-047, MS05-049, MS05-050, MS05-051, and MS05-052 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: MS05-044, MS05-045, MS05-047, MS05-049, MS05-050, MS05-051, and MS05-052 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: MS05-044, MS05-045, MS05-047, MS05-049, MS05-050, MS05-051, and MS05-052 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:

MS05-044 Vulnerability in the Windows FTP Client Could Allow File Transfer Location Tampering (905495): A tampering vulnerability exists in the Windows FTP client. This vulnerability could allow an attacker to modify the intended destination location for a file transfer, when a client has manually chosen to transfer a file by using FTP. This vulnerability could allow the attacker to write the file to any file system that is located on an affected system. This vulnerability impacts S8100/DefinityOne/IP600 Media Servers, Messaging Application Server (MAS), and Unified Communication Center. The Common Vulnerabilities and Exposures website (cve.mitre.org) has assigned the name CAN-2005-2126 to this issue.

MS05-045 Vulnerability in Network Connection Manager Could Allow Denial of Service (905414): A denial of service vulnerability exists that could allow an attacker, with valid logon credentials, to send a specially crafted network packet to an affected system. An attacker who successfully exploited this vulnerability could cause the component responsible for managing network and remote access connections to stop responding. If the affected component is stopped due to an attack, it will automatically restart when new requests are received. This vulnerability impacts S8100/DefinityOne/IP600 Media Servers, Messaging Application Server (MAS), and Unified Communication Center. The Common Vulnerabilities and Exposures website (cve.mitre.org) has assigned the name CAN-2005-2307 to this issue.

MS05-046 Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution (899589): A remote code execution vulnerability exists in the Client Service for NetWare (CSNW) that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system. Avaya System Products do not have Client Service for NetWare (CSNW) installed and therefore are not affected by this vulnerability. The Common Vulnerabilities and Exposures website (cve.mitre.org) has assigned the name CAN-2005-1985 to this issue.

MS05-047 Vulnerability in Plug and Play Could Allow Remote Code Execution and Local Elevation of Privilege (905749): A remote code execution and local elevation of privilege vulnerability exists in Plug and Play that could allow an authenticated attacker who successfully exploited this vulnerability to take complete control of the affected system. If the security updates that are provided by Microsoft Security Bulletin MS05-039, and covered in Avaya Security Advisory ASA-2005-164, have not been installed on Avaya System Products, this issue could be exploited remotely by anonymous users. If these security updates have been installed, this issue is restricted to authenticated users on Avaya System Products. This vulnerability impacts S8100/DefinityOne/IP600 Media Servers, Messaging Application Server (MAS), and Unified Communication Center. The Common Vulnerabilities and Exposures website (cve.mitre.org) has assigned the name CAN-2005-1218 to this issue.

MS05-048 Vulnerability in the Microsoft Collaboration Data Objects Could Allow

Remote Code Execution (907245): A remote code execution vulnerability exists in Collaboration Data Objects that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system. Avaya System Products do not utilize Collaboration Data Objects, event sinks, and therefore are not affected by this vulnerability. The Common Vulnerabilities and Exposures website (cve.mitre.org) has assigned the name CAN-2005-1987 to this issue.

MS05-049 Vulnerabilities in Windows Shell Could Allow Remote Code Execution (900725): Multiple remote code execution vulnerability exists in Windows because of the way that it handles the .lnk file name extension and in the way that Web View in Windows Explorer handles certain HTML characters in preview fields. By persuading a user to open a malicious file, an attacker could execute code. These vulnerabilities impacts S8100/DefinityOne/IP600 Media Servers, Messaging Application Server (MAS), and Unified Communication Center. The Common Vulnerabilities and Exposures website (cve.mitre.org) has assigned the names CAN-2005-2122, CAN-2005-2118, and CAN-2005-2117 to this issue.

MS05-050 Vulnerability in DirectShow Could Allow Remote Code Execution (904706): A remote code execution vulnerability exists in DirectShow that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system. This vulnerability impacts S8100/DefinityOne/IP600 Media Servers, Messaging Application Server (MAS), and Unified Communication Center. The Common Vulnerabilities and Exposures website (cve.mitre.org) has assigned the name CAN-2005-2128 to this issue.

MS05-051 Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution (902400): Remote code execution and local elevation of privilege vulnerabilities exists in the Microsoft Distributed Transaction Coordinator and COM+ that could allow an attacker who successfully exploited these vulnerabilities to take complete control of the affected system. In addition to remote code execution vulnerabilities, multiple denial of service vulnerabilities exist that could allow an attacker to send a specially crafted network message to an affected system. An attacker could cause the Microsoft Distributed Transaction Coordinator (MSDTC) to stop responding. This vulnerability impacts S8100/DefinityOne/IP600 Media Servers, Messaging Application Server (MAS), and Unified Communication Center. The Common Vulnerabilities and Exposures website (cve.mitre.org) has assigned the names CAN-2005-2119, CAN-2005-1978, CAN-2005-1979, and CAN-2005-1980 to these issues.

MS05-052 Cumulative Security Update for Internet Explorer (896688): A remote code execution vulnerability exists in the way Internet Explorer instantiates COM objects that are not intended to be instantiated in Internet Explorer. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited the malicious Web site. 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. The Common Vulnerabilities and Exposures website (cve.mitre.org) has assigned the name CAN-2005-2127 to this issue.

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 - October 11, 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.