

Windows Security Updates for January 2005 - (MS05-001 - MS05-003)

Advisory Original Release Date: January 12, 2005

Last Revised: January 12, 2005

Number: ASA-2005-004

Risk Level: Low

Advisory Version: 1.0

Advisory Status: Final

Overview: Microsoft issued a security bulletin summary for January 2005 which contained three security advisories: MS05-001, MS05-002, and MS05-003. 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/200501_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 MS05-001, MS05-002, and MS05-003 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/MS05-001.mspx>

<http://www.microsoft.com/technet/security/bulletin/MS05-002.mspx>

<http://www.microsoft.com/technet/security/bulletin/MS05-003.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	All Versions

Reporting Desktop – server	
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
S3400 Modular Messaging	All Versions	Follow Microsoft's recommendation for installing the Operating System patches: MS05-001, MS05-002, and MS05-003. The S3400 Modular Messaging product is deployed with the Microsoft Windows 2000 Operating System.
Messaging Application Server (MAS)	All Versions	Follow Microsoft's recommendation for installing the Operating System patches: MS05-001, MS05-002, and

		MS05-003. 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: MS05-001, MS05-002, and MS05-003. The issue described in MS05-003 does not impact this product because the Indexing Service is not enabled. 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:

MS05-001 This vulnerability impacts Internet Explorer and applies to S8100/DefinityOne/IP600 Media Servers, Messaging Application Server (MAS), and S3400 Modular Messaging. This vulnerability could allow a remote attacker to execute arbitrary code. An attacker who successfully exploited this vulnerability could gain the same privileges as the user.

MS05-002 Microsoft cursor and icon format handling contains two separate vulnerabilities. These vulnerabilities affect the S8100/DefinityOne/IP600 Media Servers, Messaging Application Server (MAS), and S3400 Modular Messaging. These vulnerabilities could allow a remote attacker to execute arbitrary code via a specially crafted cursor or icon file. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

MS05-003 The Indexing Service for Microsoft Operating Systems contains a vulnerability. This vulnerability affects Modular Messaging S3400 and the Messaging Application Server (MAS). Both Modular Messaging S3400 and MAS

requiring a manual start, the Indexing Service is not accessible from Internet Information Server. Therefore only local authenticated users would be able to attempt to exploit this vulnerability and only after the Indexing Service has been manually started.

Although Avaya S8100/DefinityOne/IP600 Media Servers do not ship with the Indexing Service enabled, and are therefore not affected by this vulnerability, Microsoft recommends Windows 2000 systems apply this update for an additional security-related change.

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 – January 12, 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.