
MS06-073 Vulnerability in Visual Studio 2005 Could Allow Remote Code Execution (925674)

Original Release Date: December 12, 2006

Last Revised: December 12, 2006

Number: ASA-2006-271

Risk Level: None

Advisory Version: 1.0

Advisory Status: Final

1. Overview:

Microsoft issued a security bulletin which contained security advisory: MS06-073. The advisory describes a vulnerability in Visual Studio 2005. A remote code execution vulnerability exists in the WMI Object Broker control that the WMI Wizard uses in Visual Studio 2005. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code execution if a user viewed the Web page. An attacker who successfully exploited this vulnerability could take complete control of the affected system. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name [CVE-2006-4704](https://cve.mitre.org/cve/2006/4704) to this issue.

A description of the vulnerability can be found at:

- <http://www.microsoft.com/technet/security/bulletin/ms06-073.msp>

2. Avaya System Products with Visual Studio 2005: None.

3. 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 that 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 vulnerability directly but the underlying Microsoft Windows platform may be. For affected Microsoft Operating Systems, Microsoft recommends installing patches. Detailed instructions for patching the Operating System are given by Microsoft at the following links:

4. Software-Only Products:

Product:	Software Version(s):
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 Contact Center Express (ACCE)	All Versions
Avaya CVLAN Client	All Versions
Avaya Enterprise Manager	All Versions
Avaya Integrated Management	All Versions
Avaya Interaction Center (IC)	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(r) Server	All Versions
Avaya OctelDesignerTM	All Versions
Avaya Operational Analyst	All Versions
Avaya Outbound Contact Management	All Versions
Avaya Speech Access	All Versions
Avaya Unified Communication Center (UCC)	All Versions

Avaya Unified Messenger (r)	All Versions
Avaya Visual Messenger TM	All Versions
Avaya Visual Vector Client	All Versions
Avaya VPNmanagerTM Console	All Versions
Avaya Web Messenger	All Versions

Recommended Actions:

Avaya recommends that customers follow recommended actions supplied by Microsoft Windows or remove the affected package.

5. Additional Information:

Additional information may also be available via the Avaya support [website](#) and through your Avaya account representative. Please contact your Avaya product support representative, or dial 1-800-242-2121, with any questions.

6. 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.

7. Revision History:

V 1.0 - December 12, 2006 - 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.

© 2006 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.