Concerning Microsoft Security Bulletin MS03-039 Buffer Overrun In RPCSS Service

Advisory Original Release Date: September 12, 2003
Last Revised: September 12, 2005
Number: 03-6
Advisory Version: 1.1

Advisory Status: Final

Overview:
The recent Microsoft Security Bulletin MS03-039 concerning "Buffer Overrun In RPCSS Service Could Allow Code Execution" affects the operating system underlying certain Avaya™ products. Action may be necessary to protect the operating system underlying these products from being exploited.

Recommended Actions:
To limit the possibility of the vulnerability being exploited from outside of the enterprise network it is a good practice to restrict access at the enterprise firewall by blocking traffic on well known RPC ports as recommended in http://www.cert.org/advisories/CA-2003-23.html

When applying operating system patches always follow best practices as described by the operating system vendor. Generally best practices include backing-up critical data, preparing a back out plan, and targeting least critical servers first. Contact your Avaya product support representative with any questions concerning Avaya products.

Avaya Software-Only Products
Avaya software-only products operate on general-purpose operating systems. Occasionally a vulnerability may be discovered in the underlying operating system that does not impact the product directly but may threaten the integrity of the underlying platform. In the case of MS03-039, Avaya software-only products are not affected by the vulnerability but the underlying Microsoft platform may be, as described in Microsoft Security Bulletin MS03-039.

Microsoft recommends administrators install the operating system patch described at <Microsoft Security Bulletin MS03-039>.

The following Avaya software-only products run on Microsoft operating systems:

Avaya software-only product	S/W Version
Avaya Basic Call Management System Reporting Desktop	All versions
Avaya CMS Supervisor	All versions
Avaya Integrated Management	All versions
Avaya Interaction Center	All versions
Avaya IP Agent	All versions

Avaya IP Softphone	All versions
Avaya Message Manager	All versions
Avaya Operational Analyst	All versions
Avaya Unified Communication Center	All versions
Avaya Unified Messenger®	All versions
Avaya VPNmanager™ Console	All versions
Avaya Web Messenger	All versions
Avaya Enterprise Manager	All versions

Avaya System Products

Avaya system products include an operating system with the product. Microsoft recommends that administrators install the operating system patch described at <Microsoft Security Bulletin MS03-039>. Please contact your Avaya product support representative with any questions about these actions.

Avaya product	Affected S/W Version	Actions
Avaya S3400 Modular Messaging	All versions	Follow Microsoft's recommendation for installing the operating system patch described at <Microsoft Security Bulletin MS03-039>.
Avaya S8100/ Definity One/ IP600 Media Server	All Versions	Once the patch is applied to the S8100/ DefinityOne/ IP600, DO NOT ALLOW the patch to reboot the system and/or DO NOT reboot the system from the desktop. You must perform a "graceful" shutdown of the system using the Web Interface or the BASH command "reboot nice". See product documentation on detailed information for these procedures. Follow Microsoft's recommendation for installing the operating system patch described at <Microsoft Security Bulletin MS03-039>.

Additional Information: Additional information may be available via the Avaya support website (http://support.avaya.com) and through your Avaya account representative.

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED "AS IS". AVAYA INC. DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA INC. MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS' SYSTEMS.IN NO EVENT SHALL AVAYA INC. 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 INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Revision History:

V 1.0 - September 12, 2003 - Initial statement issued.
V 1.1 - September 12, 2005 - Changed advisory status.

See http://support.avaya.com/security for the latest status of this advisory.

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