Zotob Worm Advisory

Advisory Original Release Date: August 17, 2005
Last Revised: August 17, 2005
Number: ASA-2005-166
Risk Level: High
Advisory Version: 1.0

Advisory Status: Final

Overview: A worm, known as Zotob, was recently found in the wild infecting unpatched Windows 2000 systems. This worm, and its variants, exploits a vulnerability in Microsoft Universal Plug and Play (UPnP) which was addressed by Microsoft Security Bulletin MS05-039. Zotob installs malicious software, and then searches for other systems to infect. Avaya has received reports of Avaya products being infected with the Zotob worm. Earlier this month Avaya released an advisory, ASA-2005-164, regarding MS05-039 and advised affected customers to install the Microsoft patch. ASA-2005-164, entitled Windows Security Updates for August 2005 – (MS05-038-MS05-043), can be viewed at:

http://support.avaya.com/elmodocs2/security/ASA-2005-164.pdf

Customers who have installed the MS05-039 patch are protected from Zotob and its variants.

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 the steps provided in the recommended actions section below. The Unified Communications Center product is deployed with the Microsoft Windows 2000 Operating System.
Modular Messaging - Messaging Application Server (MAS)	All Versions	Follow the steps provided in the recommended actions section below. The Modular Messaging - Messaging Application Server (MAS) is deployed with the Microsoft Windows 2000 Operating System.
S8100/DefinityOne/IP600 Media Servers	All Versions	Follow the steps provided in the recommended actions section below.

		These products are deployed with either the Microsoft Windows 2000 Operating System or the Microsoft Windows NT Operating System.

Recommended Actions: Avaya recommends that customers download and install the Microsoft MS05-039 patch to the Avaya System Products outlined in the above table. The MS05-039 patch is available at:

http://www.microsoft.com/technet/security/bulletin/MS05-039.mspx

Customers suspecting a Zotob, or variant, infection should utilize the information provided by Microsoft to identify and remove the worm. Microsoft's instructions for checking if a system is infected with Zotob are located at:

http://www.microsoft.com/security/incident/zotob.mspx

Microsoft's malicious software removal tool can be used to remove Zotob from infected systems:

http://www.microsoft.com/security/malwareremove/default.mspx#run

Customers may also call Avaya Global Technical Services (GTS) for assistance installing MS05-039 and remediating Zotob on affected Avaya System Products. A service ticket may be opened by calling 1-800-242-2121 and following the voice prompts. Please be aware that charges may apply.

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 1-800-242-2121, 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 - August 17, 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.