MS07-067 Vulnerability in Macrovision Driver Could Allow Local Elevation of Privilege (944653)

Original Release Date: December 12, 2007
Last Revised: December 12, 2007
Number: ASA-2007-511
Risk Level: Low
Advisory Version: 1.0
Advisory Status: Final

1. Overview:

Microsoft issued a security bulletin which contained security advisory MS07-067. This security update resolves an issue where a local elevation of privilege vulnerability exists in the way that the Macrovision driver incorrectly handles configuration parameters. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2007-5587 to this issue. A description of the vulnerability may be found at:

- http://www.microsoft.com/technet/security/bulletin/ms07-067.mspx

Certain Avaya products utilize Microsoft Operating Systems and may be affected by this vulnerability.

2. 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 Version(s):**	**Risk Level:**	**Actions:**
Avaya Messaging Application Server	All	Low	Avaya recommends that customers install the security update as provided via Microsoft Windows Update.

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 link:

- http://www.microsoft.com/technet/security/bulletin/ms07-067.mspx

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 Customer Interaction Express (CIE)	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 install the security update as provided via Microsoft Windows update.

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 BUT NOT LIMITED TO 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, INCIDENTAL, STATUTORY, 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, 2007 - 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.