flash-plugin security update (RHSA-2009-0334)

Original Release Date: February 27, 2009
Last Revised: February 27, 2009
Number: ASA-2009-066
Risk Level: None
Advisory Version: 1.0
Advisory Status: Final

1. Overview:

The flash-plugin package contains a Firefox-compatible Adobe Flash Player Web browser plug-in.

Multiple input validation flaws were found in the way Flash Player displayed certain SWF (Shockwave Flash) content. An attacker could use these flaws to create a specially-crafted SWF file that could cause flash-plugin to crash, or, possibly, execute arbitrary code when the victim loaded a page containing the specially-crafted SWF content. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the names CVE-2009-0520 and CVE-2009-0519 to these issues.

No Avaya system products are vulnerable, as flash-plugin is not installed by default.

More information about these vulnerabilities can be found in the security advisory issued by RedHat Linux:

- https://rhn.redhat.com/errata/RHSA-2009-0334.html

2. Avaya System Products with flash-plugin installed: 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 Linux platform may be. Customers should

determine on which Linux operating system the product was installed and then follow that vendor's guidance.

Product:	Actions:
CVLAN	Depending on the Operating System provided by customers, the affected package may be installed on the underlying Operating System supporting the CVLAN application.
Avaya Integrated Management Suite (IMS)	Depending on the Operating System provided by customers, the affected package may be installed on the underlying Operating System supporting the IMS application.
Voice Portal	Depending on the Operating System provided by customers, the affected package may be installed on the underlying Operating System supporting the Voice Portal application.
AES 4.x	Depending on the Operating System provided by customers, the affected package may be installed on the underlying Operating System supporting the AES application.

Recommended Actions:
In the event that the affected package is installed, Avaya recommends that customers follow recommended actions supplied by RedHat Linux.

4. 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.

5. 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.

6. Revision History:

V 1.0 - February 27, 2009 - 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.