net-snmp security update (RHSA-2008-0971)

Original Release Date: December 9, 2008
Last Revised: May 13, 2009
Number: ASA-2008-467
Risk Level: Low
Advisory Version: 2.0
Advisory Status: Interim

1. Overview:

The Simple Network Management Protocol (SNMP) is a protocol used for network management.

A denial-of-service flaw was found in the way Net-SNMP processes SNMP GETBULK requests. A remote attacker who issued a specially-crafted request could cause the snmpd server to crash. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CVE-2008-4309 to this issue.

Note: An attacker must have read access to the SNMP server in order to exploit this flaw. In the default configuration, the community name "public" grants read-only access. In production deployments, it is recommended to change this default community name.

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

- https://rhn.redhat.com/errata/RHSA-2008-0971.html

2. Avaya System Products with net-snmp installed:

Product:	**Affected Version(s):**	**Risk Level:**	**Actions:**
Avaya AES	3.1.6, 4.2.1	Low	See recommended actions below. This issue will be addressed in accordance with Avaya's Product Security Vulnerability Response Policy
Avaya Communication Manager	All	Low	Upgrade to CM 5.2 or later.
Avaya Intuity AUDIX LX	All	Low	See recommended actions below. This issue will be addressed in accordance with Avaya's Product Security Vulnerability Response Policy
Avaya EMMC	All	Low	Will not be addressed since no further releases of EMMC are planned.
Avaya Messaging Storage Server	All	Low	See recommended actions below. This issue will be addressed in accordance with Avaya's Product Security Vulnerability Response Policy
Avaya Message Networking	All	Low	See recommended actions below. This issue will be addressed in accordance with Avaya's Product Security Vulnerability Response Policy

Avaya SIP Enablement Services	5.1.2	Low	Upgrade to SES 5.2 or later.

Recommended Actions:
For all vulnerable system products, Avaya recommends that customers restrict local and network access to the server. This restriction should be enforced through the use of physical security, firewalls, ACLs, VPNs, and other generally-accepted networking practices until such time as an update becomes available and can be installed.

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.

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 - December 9, 2008 - Initial Statement issued.
V 2.0 - May 13, 2009 - Changed CM and SES actions.

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