# Vulnerabilities in krb5 - (RHSA-2005-330)

**Advisory Original Release Date:** April 27, 2005
**Last Revised:** May 3, 2005
**Number:** ASA-2005-088
**Risk Level:** Low
**Advisory Version:** 1.1

**Advisory Status:** Final

**Overview:**

Kerberos is a networked authentication system which uses a trusted third party (a KDC) to authenticate clients and servers to each other.

Multiple security vulnerabilities were discovered in the Kerberos 5 telnet client. The most serious of these vulnerabilities could allow an attacker to run arbitrary code if the victim can be tricked into connecting to a malicious telnet server using the Kerberos-aware telnet client. Certain Avaya products include vulnerable versions of Kerberos. However, by default these products do not utilize the Kerberos telnet client. Therefore Avaya does not believe these vulnerabilities are exploitable.

More information about this vulnerability can be found in the security advisories issued by Red Hat:

* https://rhn.redhat.com/errata/RHSA-2005-330.html

**Recommended Actions:** Avaya recommends that user-level access be restricted to authorized personal only and that the Kerberos telnet client not be utilized.

**System Products which contain krb5:**

| Product | Affected S/W Version | Actions |
|---|---|---|
| Avaya™ S8700/S8500/S8300 | CM2.0 and later | Follow the recommended actions above. |
| Avaya™ MN100 | All versions | Follow the recommended actions above. |
| Avaya™ Intuity LX | 1.1-5.x | Follow the recommended actions above. |
| Avaya™ Modular Messaging MSS | All versions | Follow the recommended actions above. |
| Avaya™ MN100 | All versions | Follow the recommended actions above. |

## 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 vendors guidance:

**Software-Only Products**

| Product | Affected S/W Version | Actions |
| --- | --- | --- |
| Avaya™ CVLAN | All versions | Depending on the Operating System provided by customers, Kerberos may be installed on the underlying Operating System supporting the CVLAN application. The CVLAN application does not require Kerberos. Avaya recommends that customers follow recommended actions supplied by the Operating System vendor (e.g. Red Hat) or remove the affected package(s). |

**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 1-866-GO-AVAYA, 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 – April 27, 2005 – Initial statement issued.
V 1.1 – May 3, 2005 – Fixed typo in Red Hat link.

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