Vulnerabilities in krb5 - (RHSA-2004-448) & (RHSA-2004-350)

Advisory Original Release Date: September 9, 2004
Last Revised: February 8, 2005
Number: ASA-2004-039
Risk Level: Low
Advisory Version: 2.0

Advisory Status: Final

Overview:

Multiple security vulnerabilities were discovered in Kerberos 5 and Kerberos libraries. The most serious of these vulnerabilities could allow an attacker to run arbitrary code. Certain Avaya products include vulnerable versions of Kerberos. However, by default these products do not utilize Kerberos, nor is it enable or accessible, in any network services. Additionally, no setuid or setgid packages on these products utilize the Kerberos libraries. 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-2004-448.html> <https://rhn.redhat.com/errata/RHSA-2004-350.html>.

Recommended Actions: Avaya recommends that user-level access be restricted to authorized personal only.

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™ Converged Communication Server	All versions	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 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 RHSA-2004-448 and RHSA-2004-350 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).
Avaya™ Integrated Management	All versions	Depending on the Operating System provided by customers, Kerberos may be installed on the underlying Operating System supporting the Integrated Management application. The Integrated Management application does not require Kerberos. Avaya recommends that customers follow recommended actions supplied by the Operating System vendor (e.g. Red Hat).

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.

Revision History:

V 1.0 – September 9, 2004 – Initial statement issued.
V 2.0 – February 8, 2005 – Added MN100, MSS, and Intuity LX to system products.

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