Vulnerabilities in Linux Kernel - (RHSA-2005-016/017 & RHSA-2005-043)

Advisory Original Release Date: February 8, 2005
Last Revised: November 8, 2005
Number: ASA-2005-034
Risk Level: Medium
Advisory Version: 2.1

Advisory Status: Interim

Overview:

Multiple security vulnerabilities were discovered in the Linux kernel. These vulnerabilities could allow local users to cause a denial of server (DoS) and possibly execute arbitrary code on affected system. Certain Avaya products utilize the Linux kernel and are therefore affected by some of these vulnerabilities.

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

- https://rhn.redhat.com/errata/RHSA-2005-016.html
- https://rhn.redhat.com/errata/RHSA-2005-017.html
- https://rhn.redhat.com/errata/RHSA-2005-043.html

Recommended Actions for Communication Manager:

Avaya recommends that customers upgrade to Communication Manager 2.2.1 or 3.0 (or later) to take advantage of these and other security fixes.

Recommended Actions:

For all system products which use vulnerable versions of the Linux kernel, Avaya recommends that customers restrict local 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.

System Products utilizing Linux Kernel 2.4.x:

Product	Affected S/W Version	Actions	Risk Level
Avaya™ S8710/S8700/ S8500/S8300	All versions prior to CM2.2.1 or CM3.0	Avaya recommends that customers upgrade to CM 2.2.1 or 3.0 (or later) to take advantage of these, and other, security updates. Avaya™ S8710/S8700/S8500/S8300 products are affected by the	Medium

		following vulnerabilities: CAN-2004-1235	
Avaya™ Converged Communication Server	All versions	Follow the recommended actions above until an update becomes available and can be installed. An update is being considered for a future release. Avaya™ Converged Communications Server is affected by the following vulnerabilities: CAN-2004-1235	Medium
Avaya™ Intuity LX	All versions	Follow the recommended actions above until an update becomes available and can be installed. An update is being considered for a future release. Avaya™ Intuity LX is affected by the following vulnerabilities: CAN-2004-1057, CAN-2004-1235, and CAN-2005-0003	Medium
Avaya™ MN100	All versions	Follow the recommended actions above until an update becomes available and can be installed. An update is being considered for a future release. Avaya™ MN100 is affected by the following vulnerabilities: CAN-2004-1057, CAN-2004-1235, and CAN-2005-0003	Medium
Avaya™ Modular Messaging - MSS	All versions	Follow the recommended actions above until an update becomes available and can be installed. An update is being considered for a future release. Avaya™ Modular Messaging - MSS is affected by the following vulnerabilities: CAN-2004-1057, CAN-2004-1235, and CAN-2005-0003	Medium

Avaya™ Network Routing (ANR)	All versions	Follow the recommended actions above until an update becomes available and can be installed. An update is being considered for a future release. Avaya™ Network Routing (ANR) is affected by the following vulnerabilities: CAN-2004-1057, CAN-2004-1235, and CAN-2005-0003	Medium

Further information regarding the Linux kernel vulnerabilities on Avaya system products is below:

CAN-2004-1016: Avaya previously addressed this issue in ASA-2005-006.

CAN-2004-1017: Avaya previously addressed this issue in ASA-2005-006.

CAN-2004-1057: Certain drivers in the Linux kernel are missing VM_IO flags. This could lead to a memory leak vulnerability. This vulnerability affects Avaya system products including Network Routing, MN100, Modular Messaging MSS, and Intuity LX.

CAN-2004-1234: Avaya previously addressed this issue in ASA-2005-006.

CAN-2004-1235: Avaya previously addressed this issue in ASA-2005-006.

CAN-2004-1335: Avaya previously addressed this issue in ASA-2005-006.

CAN-2005-0001: A vulnerability in the page fault handler (fault.c) for Linux kernels could allow local users to execute arbitrary code. This vulnerability only affects multiprocessor (SMP) systems. Avaya system products do not operating on multiprocessor systems and therefore are not affected by this vulnerability.

CAN-2004-1235: A vulnerability in the uselib(2) system call in Linux kernels could allow local users to gain elevated (root) privileges. This vulnerability affects Avaya system products including S8710/S8700/S8500/S8300, Converged Communications Server, Network Routing, MN100, Modular Messaging MSS, and Intuity LX.

CAN-2004-1237: A vulnerability was discovered in the system call filtering code of the audit subsystem. This vulnerability could allow local users to cause a denial of service on systems with auditing enabled. Avaya system products do not apply the audit subsystem to product kernels and therefore are not affected by this vulnerability.

CAN-2005-0003: A vulnerability in ELF and a.out binary support in Linux kernels was discovered. This vulnerability could allow local users to cause a denial of

service (system crash) or execute arbitrary code via a specially crafted ELF or a.out file which causes overlapping VMA (virtual memory address) allocations. This vulnerability affects Avaya system products including Network Routing, MN100, Modular Messaging MSS, and Intuity LX.

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-2005-016, RHSA-2006-017, and RHSA-2005-043 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 hardware and Operating System provided by customers, the above Linux kernel vulnerabilities may affect CVLAN. 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 1-800-242-2121, 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 - February 8, 2005 - Initial statement issued.
V 2.0 - October 31, 2005 - Added information about CM 3.0.
V 2.1 - November 8, 2005 - Added information about CM 2.2.1

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