Vulnerabilities in Linux Kernel - (RHSA-2005-283/284, RHSA-2005-293/294 & RHSA-2005-472)

Advisory Original Release Date: June 2, 2005
Last Revised: June 3, 2005
Number: ASA-2005-120
Risk Level: Medium
Advisory Version: 2.0

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 these vulnerabilities can be found in the security advisories issued by Red Hat

- https://rhn.redhat.com/errata/RHSA-2005-283.html
- https://rhn.redhat.com/errata/RHSA-2005-284.html
- https://rhn.redhat.com/errata/RHSA-2005-293.html
- https://rhn.redhat.com/errata/RHSA-2005-294.html
- https://rhn.redhat.com/errata/RHSA-2005-472.html

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	Follow the recommended actions above until an update becomes available and can be installed. An update is being considered for a future release. Avaya™ S8710/S8700/S8500/S8300 products are affected by the following vulnerabilities: CAN-2004-0814, CAN-2004-1058, CAN-	Medium

		2005-0384, CAN-2005-0449, CAN-2005-0749, and CAN-2005-1263	
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-2004-0814, CAN-2004-1058, CAN-2005-0384, CAN-2005-0449, CAN-2005-0749, and CAN-2005-1263	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-2004-0814, CAN-2004-1058, CAN-2005-0384, CAN-2005-0449, CAN-2005-0749, and CAN-2005-1263	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-2004-0814, CAN-2004-1058, CAN-2005-0384, CAN-2005-0449, CAN-2005-0749, and CAN-2005-1263	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-2004-0814, CAN-2004-1058, CAN-2005-0384, CAN-2005-0449, CAN-2005-0749, and CAN-2005-1263	Medium

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

CAN-2004-0075: The Vicam USB driver in Linux before 2.4.25 does not use the copy_from_user function when copying data from userspace to kernel space, which crosses security boundaries and allows local users to cause a denial of service. Avaya system products do not utilize the Vicam USB driver, and therefore are not affected by this vulnerability.

CAN-2004-0177: This issue has been previously addressed in ASA-2005-006.

CAN-2004-0491: The linux-2.4.21-mlock.patch in Red Hat Enterprise Linux 3 does not properly maintain the mlock page count when one process unlocks pages that belong to another process, which allows local users to mlock more memory than specified by the rlimit. Avaya system products do not run the RHEL 3 kernel, and therefore are not affected by this vulnerability.

CAN-2004-0619: This issue has been previously addressed in ASA-2005-006.

CAN-2004-0814: The terminal layer in Linux kernels 2.4.x and 2.6.x before 2.6.9 did not properly lock line discipline changes or pending IO. An unprivileged local user could read portions of kernel memory, or cause a denial of service (system crash). This vulnerability affects the Avaya system products including: S8700/S8710/S8500/S8300, Converged Communication Server (CCS), Modular Messaging MSS, MN100, and Intuity LX

CAN-2004-1058: A race condition was discovered affecting 2.4.x and 2.6.x Linux kernels. Local users could use this flaw to read the environment variables of another process that is still spawning via /proc/.../cmdline. This vulnerability affects the Avaya system products including: S8700/S8710/S8500/S8300, Converged Communication Server (CCS), Modular Messaging MSS, MN100, and Intuity LX.

CAN-2004-1073: This issue has been previously addressed in ASA-2005-006.

CAN-2005-0135: A flaw was discovered in the Itanium (ia64) kernel unw_unwind_to_user() function. A local user could use this flaw to cause a denial of service (system crash) on the Itanium architecture. Avaya system products do not utilize the Itanium (ia64) kernels, and therefore are not affected by this vulnerability.

CAN-2005-0137: A missing Itanium (ia64) kernel syscall table entry could allow an unprivileged local user to cause a denial of service (system crash) on the Itanium architecture. Avaya system products do not utilize the Itanium (ia64) kernels, and therefore are not affected by this vulnerability.

CAN-2005-0176: A flaw in the Linux 2.6.9 kernel was found in shared memory locking which allowed local unprivileged users to lock and unlock regions of shared memory segments they did not own. Avaya system products do not run the Linux 2.6.9 kernel, and therefore are not affected by this vulnerability.

CAN-2005-0204: A flaw affecting the OUTS instruction on the AMD64 and Intel EM64T architectures was discovered. A local user could use this flaw to access privileged IO ports. Avaya system products do not utilize the AMD64 or EM64T architectures, and therefore are not affected by this vulnerability.

CAN-2005-0384: A flaw was discovered in the Linux PPP driver. On systems allowing remote users to connect to a server using ppp, a remote client could cause a denial of service (system crash). This vulnerability affects the Avaya system products including: S8700/S8710/S8500/S8300, Converged Communication Server (CCS), Modular Messaging MSS, MN100, and Intuity LX.

CAN-2005-0403: A flaw in the Red Hat backport of NPTL to Red Hat Enterprise Linux 3 was discovered that left a pointer to a freed tty structure. A local user could potentially use this flaw to cause a denial of service (system crash) or possibly gain read or write access to ttys that should normally be prevented. Avaya system products do not run the RHEL 3 kernel, and therefore are not affected by this vulnerability.

CAN-2005-0449: A flaw in fragment queuing was discovered affecting the netfilter subsystem. On systems configured to filter or process network packets a remote attacker could send a carefully crafted set of fragmented packets to a machine and cause a denial of service (system crash). In order to successfully exploit this flaw, the attacker would need to know (or guess) some aspects of the firewall ruleset in place on the target system to be able to craft the right fragmented packets. This vulnerability affects the Avaya system products including: S8700/S8710/S8500/S8300, Converged Communication Server (CCS), Modular Messaging MSS, MN100, and Intuity LX.

CAN-2005-0736: Missing validation of an epoll_wait() system call parameter could allow a local user to cause a denial of service (system crash) in the Linux 2.6 kernel. Avaya system products do not run the Linux 2.6 kernel, and therefore are not affected by this vulnerability.

CAN-2005-0749: A flaw when freeing a pointer in load_elf_library was discovered. A local user could potentially use this flaw to cause a denial of service (system crash). This vulnerability affects the Avaya system products including: S8700/S8710/S8500/S8300, Converged Communication Server (CCS), Modular Messaging MSS, MN100, and Intuity LX.

CAN-2005-0750: A flaw was discovered in the bluetooth driver system. On system where the bluetooth modules are loaded, a local user could use this flaw to gain elevated (root) privileges. Avaya system products do not utilize bluetooth modules, and therefore are not affected by this vulnerability.

CAN-2005-0757: A flaw in offset handling in the xattr file system code backported to Red Hat Enterprise Linux 3 was fixed. On 64-bit systems, a user who can access an ext3 extended-attribute-enabled file system could cause a denial of service (system crash). Avaya system products do not run the RHEL 3 kernel, and therefore are not affected by this vulnerability.

CAN-2005-1263: A flaw between execve() syscall handling and core dumping of ELF-format executables allowed local unprivileged users to cause a denial of service (system crash) or possibly gain privileges. This vulnerability affects the

Avaya system products including: S8700/S8710/S8500/S8300, Converged Communication Server (CCS), Modular Messaging MSS, MN100, 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 these advisories 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).
Avaya Integrated Management/ System Management (IM/SM)	Advanced Offer	Depending on the hardware and Operating System provided by customers, the above Linux kernel vulnerabilities may affect IM/SM. 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.

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 - June 2, 2005 - Initial statement issued.
V 2.0 - June 3, 2005 - Added RHSA-2005-294.

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