Simple Network Management Protocol (SNMP) Vulnerabilities in Multiple Avaya Products

Advisory Original Release Date: March 6, 2002
Last Revised: October 30, 2002
Advisory Version: 1.14 (see bottom for revision history)

Advisory Status: Interim. Updates are expected as more information becomes available. Updates may include additional products added to the list of affected products, below, or additional information, such the availability and location of a fix.

Overview: The Computer Emergency Response Team Coordination Center (CERT/CC) issued an advisory (CA-2002-03, http://www.cert.org/advisories/CA-2002-03.html) that outlines the availability of a protocol testing tool, PROTOS, from the Oulu University Secure Programming Group (http://www.ee.oulu.fi/research/ouspg/) that may be used by malicious users to attack susceptible networked systems via the SNMP protocol (http://www.ee.oulu.fi/research/ouspg/protos/testing/c06/snmpv1/index.html). Frequently Asked Questions about SNMP are available from CERT at: http://www.cert.org/tech_tips/snmp_faq.html. This advisory addresses Avaya products that are susceptible to attack via the PROTOS testing tool.

Description: The PROTOS tool does extensive protocol testing on a targeted device. The tool generates thousands of test cases of valid SNMP packets with anomalous packet contents. While no specific attacks have been reported against any Avaya products, as noted in the CERT Advisory, the potential for malicious use of these tools exists.

Impact: This vulnerability may result in unauthorized access, denial-of-service attacks, or unstable system behavior. Generally speaking only a few test cases adversely affected any particular product. While a wide variety of products are susceptible to malicious use of the tool, it is expected that firewalls should generally prevent attacks at the network perimeter from untrusted sources, thereby minimizing the potential impact.

Recommended Actions: General advice to minimize the impact of the problem before a patch or an updated version of software can be installed includes the following (more specific work-around information may be described below for a particular device):

1) Filter SNMP services at your network perimeter (ingress/egress filtering).
2) Filter SNMP access to managed devices to ensure the traffic originates from known management systems.
3) Disable the SNMP service if not necessary
4) Change SNMP community strings from their defaults values.
5) Segregate network management traffic onto a separate network.
6) Use switched network architecture.
7) Monitor SNMP usage and logs.
8) Apply patches/upgrades when available.

If the affected product is under an Avaya Services contract and *is an Avaya product*, please contact your Avaya Services personnel to discuss the best course of action. If the affected product is third party/multivendor equipment please refer to the Computer Emergency Response Team (CERT) Advisory website, http://www.cert.org/advisories/CA-2002-03.html for your product originator information and the associated advisory for that product.

Third Party / Multi-Vendor Products - Customers with third party products should obtain SNMP patches or upgraded software through their product originator or download information through the CERT website, referenced above, for security advisories. Based on the information provided in the table below, as these patches/upgrades become available please refer to Avaya's website http://support.avaya.com under your product for downloading and self-installation or contact your representative. Use our online directory for additional contact numbers: http://support.avaya.com/directories/TSO_800.jhtml. Customers whose products were purchased or maintained through prior or existing agreements with third-party support organizations such as Avaya BusinessPartners, authorized resellers, or service providers should contact that support organization for assistance.

For your specific product refer to the table below.

List of Avaya products affected:

Product	Version	Info / Status
ARIA		Until a patch is available in order to mitigate any SNMP vulnerabilities on an Aria system, administrators can do one of two things: 1. Disable responses to SNMP GET requests on the Aria system by shutting down and disabling the SNMP service/process. 2. Ensure that the Aria system is reachable only by trusted Network Management station.
CajunView		Fix will be in release 4.5 in May 2002.
Call Management System (CMS) (formerly CentreVu)	All	SNMP is enabled by default but not used by CMS. We have applied the Solaris recommended patches and procedures in our labs and they do not conflict with CMS. The patches are available for customer download from Solaris http://sunsolve.sun.com/securitypatch: 108869-15 for Solaris 8 and 107709-18 for Solaris 7. As an alternative, a customer can disable SNMP. As described in the "Customer Procedures for Securing the CMS" White Paper, available on http://support.avaya.com/ , unused network services pose a potential security risk and should be disabled. To turn off the SNMP daemon without reboot: */etc/init.d/init.snmpdx* stop Later reboots will restart SNMP unless you rename the

		initialization file: *mv /etc/init.d/S76snmpdx /etc/init.d/_S76snmpdx* Adding an underscore before the process name is our standard way to identify disabled services.
CONVERSANT ?	V6	Unixware 1.1.2 SNMP comes enabled by default, but is not used by any specific Avaya application. Caldera does not provide any patches for UW 1.1.2. No patch will be provided. If UW 1.1.2 SNMP is NOT REQUIRED to be enabled for your application, we recommend that you disable SNMP via the following command: mv/etc/rc2.d/S73snmp /etc/rc2.d/s73snmp *Note: The above command will require a system restart to take effect, or you may selectively kill the in.snmpd process currently running on your system after executing the above command.* If UW 1.1.2 SNMP is REQUIRED to be enabled for your application, we recommend that you install your CONVERSANT behind a corporate firewall to reduce the risks identified by this Security Advisory. *Please remember to consult your IVR administrator or applications developer to determine the impacts of SNMP to your application/s.*
CONVERSANT ?	V7	Unixware 2.1.2 SNMP comes enabled by default, but is not used by a specific Avaya application. Caldera has provided a patch for SNMP on UW 2.1.2. *Note: There are two forms of SNMP on CONVERSANT V7 systems: UW 2.1.2 SNMP as previously discussed, and SNMP Emanate Agent which provides custom MIBS. (Refer to your local System Reference Guide for more information on SNMP custom MIBS.)* If UW 2.1.2 SNMP is NOT REQUIRED to be enabled for your application, we recommend that you disable SNMP via the following command: *mv /etc/rc2.d/S73snmp /etc/rc2.d/s73snmp* *Note: The above command will require a system restart to take effect, or you may selectively kill the in.snmpd process currently running on your system*

		after executing the above command. If UW 2.1.2 SNMP is REQUIRED to be enabled for your application, we recommend that you install the Caldera patch. Go to http://support.avaya.com/. • Select *Call Center/CRM* • Select *Self Service* • Select *Interactive Voice Response (CONVERSANT IVR)* • Select All • Select Software Downloads • Select *CONVERSANT VIS Version 7.0 Unixware 2.1.2 SNMP CA-2002-03 Patch* To verify if SNMP Emanate Agent is currently running on your system, perform the following command: ps -ef | grep -i snmp If SNMP Emanate Agent is running, you will see any combination of the following processes returned: (compare your output with the last column only) root 13139 1 TS 49 0 13:59:26? 0:00 /vs/bin/util/snmp/cmds/snmpdm root 13140 1 TS 80 0 13:59:26 X/server.0 0:00 /vs/bin/util/snmp/cmds/mib2agt root 13141 1 TS 80 0 13:59:26 X/server.0 0:00 /vs/bin/util/snmp/cmds/csagt root 13310 1 TS 80 0 13:59:29 ? 0:01 /vs/bin/util/snmp/util/alarmMon.sh If SNMP Emanate Agent is NOT REQUIRED to be enabled for your application, we recommend you stop the Emanate Agent via the following command: */vs/bin/util/snmp/util/stopsnmp.sh* *Note: The SNMP Emanate Agent is not configured to start up automatically by default. Check with your IVR administrator or application developer to ensure that SNMP agent is not set up to restart on system boot or voice system restart.* If SNMP Emanate Agent is REQUIRED to be enabled for your application, we recommend you install the latest release of SNMP Emanate Agent. *Note: The next release of SNMP Emanate Agent to incorporate these SNMP security patches is currently under development. In the interim, we recommend that you install your CONVERSANT behind a corporate*

		firewall to reduce the risks identified by this Security Advisory. *Please remember to consult your IVR administrator or applications developer to determine the impacts of SNMP to your application/s.*
CONVERSANT ?	V8	Unixware 7.1.1 SNMP comes disabled by default, and is not used by any specific Avaya application. Caldera has provided a patch for SNMP on UW 7.1.1. *Note: There are two forms of SNMP on CONVERSANT V8 systems: UW 7.1.1 SNMP as previously discussed, and SNMP Emanate Agent which provides custom MIBS. (Refer to your local System Reference Guide for more information on SNMP custom MIBS.)* If UW 7.1.1 SNMP is NOT REQUIRED to be enabled for your application, no action is required. Your system already has Unixware SNMP disabled by default. If UW 7.1.1 SNMP is REQUIRED to be enabled for your application, we recommend that you install the Caldera patch. Go to http://support.avaya.com/. • Select *Call Center/CRM* • Select *Self Service* • Select *Interactive Voice Response (CONVERSANT IVR)* • Select *All* • Select *Software Downloads* • Select *CONVERSANT VIS Version 8.0 Unixware 7.1.1 SNMP CA-2002-03 Patch* To verify if SNMP Emanate Agent is currently running on your system, perform the following command: ps ?ef |grep ?i snmp If SNMP Emanate Agent is running, you will see any combination of the following process returned: (compare your output with the last column only) root 13139 1 TS 49 0 13:59:26 ? 0:00 /vs/bin/util/snmp/cmds/snmpdm root 13140 1 TS 80 0 13:59:26 X/server.0 0:00 /vs/bin/util/snmp/cmds/mib2agt root 13141 1 TS 80 0 13:59:26 X/server.0 0:00 /vs/bin/util/snmp/cmds/csagt root 13310 1 TS 80 0 13:59:29 ? 0:01 /vs/bin/util/snmp/util/alarmMon.sh If SNMP Emanate Agent is NOT REQUIRED to be

		enabled for your application, we recommend you stop the Emanate Agent via the following command: /vs/bin/util/snmp/util/snmpstop.sh *Note: The SNMP Emanate Agent is not configured to start up automatically by default. Check with your IVR administrator or application developer to ensure that SNMP agent is not set up to restart on system boot or voice system restart.* If SNMP Emanate Agent is REQUIRED to be enabled for your application, we recommend you install the latest release of SNMP Emanate Agent. *Note: The next release of SNMP Emanate Agent to incorporate these SNMP security patches is currently under development. In the interim, we recommend that you install your CONVERSANT behind a corporate firewall to reduce the risk of external denial of service attacks.* *Please remember to consult your IVR administrator or applications developer to determine the impacts of SNMP to your application/s.*
DEFINITY? Proxy Agent (DPA)		Coordinating with SNMP vendor for patch or upgrade.
Interchange	R4	For Interchange we recommend that customers disable SNMP if the feature is active and not being used. If you are actively using the SNMP feature, or do not wish to disable SNMP change the community string and the IP Address to a trusted Network Management station.
INTUITY™ AUDIX?	R4 (Lodging, Hicap) R5 (Lodging)	Patch is available now (04/04/02). Please contact your service representative and ask for the SNMP patch.
IP Softphone	v1, v2, v3	Although no action is specifically required for the IP Softphone, customers should consider implementing the patch released by Microsoft regarding this issue.
IP Telephone 46xx		Coordination is underway with the SNMP vendor to validate susceptibility and obtain a patch if necessary. If an SNMP patch is needed, a new version of the firmware will be released as version R1.6.1 or R1.7.
IP600		Avaya is currently implementing available patch from SNMP vendor. Avaya will be releasing a patch incorporating the new SNMP agent. Date of availability is to be determined.

Lucent Security Management Server (LSMS, Management Server for the Lucent Managed Firewall)		Until the patch is available in order to mitigate any SNMP vulnerabilities on the LSMS network administrators can do one of two things: 1. Disable responses to SNMP GET requests on the LSMS by shutting down and disabling the SNMP service/process. 2. Ensure that the LSMS is reachable only by trusted Network Management Systems.
M770 ATM	2.3.6	Fix will be in release 2.3.9, expected April 2002.
M770 Ethernet	3	Fix available in release 3.3, expected May 2002.
P120		There will no patch provided. In order to mitigate any SNMP vulnerabilities please follow the recommended actions.
P130		Fix available in release 2.8, expected April 2002.
P220	4.0	Fixes are now generally available. To access, go to http://support.avaya.com/. Then navigate to get to the software and documentation as follows: 1. Click on the link - "LAN, Backbone, and Edge Access Switches" 2. Click on the Backbone & Core General Info link for the target switch - "Avaya P882/P580 MultiService Switch" or "Avaya P550R/P880 MultiService Switch" or "Avaya P550 MultiService Switch (Discontinued)" 3. This brings you to the documentation and software download page. Note the third section, titled "Software Downloads" from which you can download the appropriate software: Avaya P882/P580 MultiService Switch: Software Release 5.2.14 or higher Avaya P550R/P880 MultiService Switch: Software Release 5.2.14 or higher Avaya P550 MultiService Switch (Discontinued): Software Release 4.3.7 or higher.
P330-ATM uplink	1.8	Fix will be available in 1.8.1, expected May 2002.
P330 Ethernet (includes P330T, P330R, P330RLB, and P330ML)		Fix is now available in release 3.9. Please refer to the Avaya Support Center.
P550, P550R, P580, P880, P882	P550 version 4.3, all	Fix now available since 5.2.13. Release 5.2.14 now generally available. To access this go to http://support.avaya.com. Then navigate two steps

	others version 5.2	to get to the documentation listing as follows: 1. Click on the link - "LAN, Backbone, and Edge Access Switches" 2. Click on the General Info link - "Avaya P882/P580 MultiService Switch" This brings you to the documentation list page, where the third section is titled "Software Downloads". Here you will find 5.2.14 code. Fix for P550 will be in version 4.3.7 is now available.
Predictive Dialing System (PDS) (formerly MOSAIX™)	9.1, 11.1, 11.2	SNMP is enabled by default but not used by PDS. We have applied the HP recommended patches/ procedures for HP-UX 10.2 and they do not conflict with PDS. http://www.cert.org/advisories/CA-2002-03.html: HPSBUX0202-184
Predictive Dialing System (PDS) (formerly MOSAIX™)	12.0	SNMP is enabled by default but not used by PDS. We have applied the HP recommended patches/ procedures for HP-UX 11 and they do not conflict with PDS. You can find the patch instructions at http://www.cert.org/advisories/CA-2002-03.html: HPSBUX0202-184
R300		Fix is currently in testing. Patch will be released under version 148.1. Date of availability is to be determined.
SERENADE?		Until a patch is available in order to mitigate any SNMP vulnerabilities on the Serenade system, administrators can do one of two things: 1. Disable responses to SNMP GET requests on the Serenade system by shutting down and disabling the SNMP service/process. 2. Ensure that the Serenade system is reachable only by trusted Network Management station.
TN2501DP		Fix is currently in testing. Patch will be released. Version and release date is to be determined.
TN799 A,B,C		A patch will be deployed as firmware V5. Will be released when testing is complete.
TN799DP		A patch will be deployed as firmware V2. Will be released when testing is complete.
VSU Gateways VSU-100, VSU-100Z, VSU-1100, VSU-1200, VSU-2000, VSU-5000, VSU-7500, VSU-10000	VPNos 3.1	The latest version of the software, 3.1.63, is not vulnerable. Previous versions are vulnerable and should be upgraded.

Additional Information: Additional information may be available via the Avaya

support website (http://support.avaya.com) and your Avaya account representative.

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS OFFERED "AS IS". AVAYA INC. IS PROVIDING THE INFORMATION CONTAINED IN THIS ADVISORY AS A HELPFUL TOOL TO CUSTOMERS. AVAYA INC. DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA INC. MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE ALL SECURITY THREATS TO THEIR SYSTEMS. IN NO EVENT SHALL AVAYA INC. BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR FIXES, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Revision History:

V1.0 - March 6, 2002 - Initial statement issued.
V1.1 - March 7, 2002 - Corrected typo on original release date of this advisory from 2001 to 2002.
V1.2 - March 11, 2002 - Added new info on CMS and PDS.
V1.3 - March 12, 2002 - Added new info on P220.
V1.4 - March 15, 2002 - Revised the statement regarding services to be less confusing.
V1.5 - March 19, 2002 - Added new information on Conversant status.
V1.6 - March 21, 2002 - Corrected errors in the first paragraph of Conversant status for V7 & V8
V1.7 - April 1, 2002 - Updated the status info on P550, P550R, P580, P880, and P882
V1.8 - April 8, 2002 - Updated the status of Intuity AUDIX R4 & R5.
V1.9 - April 17, 2002 - Updated info on Recommended Actions, Intuity AUDIX and P550-P882 status; added proper trademarks to product names.
V1.10 - May 6, 2002 - Updated status of Intuity Interchange.
V1.11 - May 17, 2002 - Added info on P120.
V1.12 - June 3, 2002 - Updated info on Conversant.
V1.13 - June 18, 2002 - Updated P550-P882 and P330 - Ethernet status, and the section on Third Party/Multi-Vendor products.
V1.14 - October 30, 2002 - Updated P220 and P550 status.

See http://support.avaya.com/security for the latest status of this advisory.

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