



TECHNICAL WHITE PAPER

Avaya™ Enterprise-Class Internet Protocol Solutions (ECLIPS) and CERT SNMP Advisory (CA2002-03)

Version: **1.6**

CID: **92078**

Issued: **February 28, 2002**

Updated: **August 9, 2002**

Author: **CES Security Team**

rickr@avaya.com

CES Converged Solutions Support Team

akkapoor@avaya.com

Scope

The scope of this paper is to provide information regarding the recommended actions that should be taken by Avaya customers who own Avaya equipment and who are concerned about the recent CERT announcement related to known SNMP vulnerabilities.

Background

On February 12, 2002 CERT/CC (Computer Emergency Response Team / Coordination Center) issued a Security Advisory (CA2002-03) that described vulnerability with common implementations of the Simple Network Messaging Protocol (SNMP). The advisory was based on information gathered from the use of a tool developed by The Oulu University Secure Programming Group in Finland (OUSPG). Detailed information about SNMP, the testing tool, and the weakness are available from CERT (www.cert.org).

Customer Recommendations

As of the time that this paper is released, developers of DEFINITY® are exercising plans to upgrade or patch all implementations of SNMP that may be susceptible to the vulnerabilities described by the CERT advisory. Most implementations of SNMP are made through the use of 3rd party software vendors and Avaya is coordinating with all of those vendors to obtain upgrades or patches to their SNMP packages.

Because the patches are being incorporated and tested concurrently with the release of this white paper, customers are asked to monitor patch availability on support.avaya.com. All patches developed by Avaya and its software vendors will be tested to ensure no reduction in product quality before they are released.

Avaya supports the customer actions recommended by CERT regarding this vulnerability. That is, in order to minimize susceptibility to this vulnerability; customers should take the following actions:

- Apply patches when available.
- Disable all nonessential SNMP software.
- Filter SNMP access to managed devices to ensure the traffic originates from known management systems.
- Filter SNMP services at your network perimeter (ingress/egress filtering).
- Change SNMP community strings from their defaults.
- Segregate network management traffic onto a separate network.

Avaya™ Enterprise-Class Internet Protocol Solutions (ECLIPS) Product status

The following table describes the state of ECLIPS products as of the time of this white paper. Avaya encourages customers to monitor support.avaya.com for more current information regarding patches and availability. If you have further questions or concerns, please feel free to contact your Avaya Service Representative.



Product	Susceptibility	Action
IP600	Evaluation shows that current implementation is susceptible to limited vulnerability. However, no information on impact of susceptibility is available at this time.	Avaya will be including an upgrade to the new SNMP agent as part of its 1.3 release. Customers are recommended to upgrade.
TN799 A,B,C	Exploitation of vulnerability suspends the SNMP task but the board continues to otherwise operate normally.	A patch was deployed as firmware V5. Customers are recommended to upgrade.
TN799DP	Exploitation of vulnerability suspends the SNMP task but the board continues to otherwise operate normally.	A patch was deployed as firmware V2. Customers are recommended to upgrade.
TN2302DP	No SNMP agent is running.	No Action Required
IP Telephone 46xx	All releases since R1.1 and prior to R1.7 are susceptible. Testing has confirmed susceptibility. Although traps are not enabled, running the Oulu Test suite revealed a memory leak on the IP Telephone.	An R1.7 release will be available in August. Customers are recommended to upgrade to R1.7, when available.
IP Softphone v1, v2, v3	IP Softphone does not expose anything through SNMP.	Although no action is specifically required for the IP Softphone, customers should consider implementing the patch released by Microsoft regarding this issue.
TN2501DP	Attack suspends the SNMP task but the board continues to otherwise operate normally.	Upgrade is available. V5 contains fix to vulnerability. V6 also contains fix and is the most current release.
R300	Device resets upon exploitation of vulnerability.	The SNMP vulnerability was fixed in release 8.0-148.1. Customers are recommended to upgrade.
DEFINITY Proxy Agent (DPA)	Evaluation shows that current implementation is susceptible to limited vulnerability. However, no information on impact of susceptibility is available at this time.	Customers should upgrade to version 4.0.0.22 or higher when available.
TN801B	SNMP not installed.	None.
TN802B	SNMP not running.	None.
TN802	SNMP not running.	None.