

Subject: SNMP_Set guessed Community Name and changed system information

7 November 2001

The following directive is issued to the PVC and VATC.

Issue: The SNMP community name is guessable, and allows anyone who can guess the name the ability to set new system information. An attacker can use SNMP to obtain valuable information about the machine, such as information on network devices and current open connections.

Fix: 1. If SNMP is needed for network management, make sure it is properly configured with private community names or change the password to something difficult to guess for the following Hosts:

PVC	VATC
198.118.220.41	198.118.232.8
198.118.220.51	198.118.232.36
198.118.220.98	198.118.232.47
198.118.220.99	198.118.232.55
198.118.220.105	198.118.232.56
198.118.220.164	198.118.232.57
	198.118.232.175
	198.118.232.179

Testing: Verify that the SNMP community name is not guessable.

Implementation: Unix: To change the community name, refer to your SNMP documentation.

--OR--

Disable SNMP if it is not needed. If SNMP is started from the rc script, comment it out.

Point of Contact: Mel Hudson, tele: 301/925-1099, email: mhudson@eos.east.hitc.com

Approved By: V. Maclin
Director, Systems Engineering

Reference CCR: 01-0860

-----End of Directive-----