Product Support Notice

PSN #	PSN003894u				
Original publication date: 16-Jan-13, This is Issue #01, published date: 16-Jan-13.		Severity/risk level	Low	Urgency	ASAP
Name of problem	Avaya 96xx, 16xx, 46xx IP Deskphone Security Recommendations				

Products affected

All Avaya 96xx, 16xx and 46xx IP Deskphones

Problem description

Mainstream news sources have reported IP telephone security vulnerability discoveries made by a private research institution conducting a study under a U.S. Defense Department grant ("Study") and documented in the Cisco Native UNIX Kernel System Call susceptibility CVE-2012-5445 ("CVE"). The kernel in Cisco Native Unix (CNU) on Cisco Unified IP Phone 7900 series devices (aka TNP phones) does not properly validate unspecified system calls, which allows attackers to execute arbitrary code or cause a denial of service (memory overwrite) via a crafted binary. Avaya products do not use Cisco Native Unix. The security weaknesses highlighted in this Study are demonstrated in instances where a serial console port is used as a means for gaining direct physical access to an IP telephone. Once access to the IP telephone is achieved, rogue files may be installed and the IP telephone may be otherwise hacked, perhaps permitting remote eavesdropping and the initiation of attacks on other devices on the network, as revealed within the reported Study.

Serial Console Port

All Avaya 96xx, 16xx and 46xx IP Deskphone models have a serial port that may function alternately as a console/debugging port. Unless this port is protected as described below, this connection may be used as a point of access. The console/debugging port is disabled by default within Avaya 96xx, 16xx and 46xx IP Deskphones thereby prohibiting the serial console port as means of access unless it is enabled. Further, to enable this port to function as a serial console port, a user must enter a password at the IP telephone dial pad, navigate an on-screen local administration menu, and then choose to enable the port to function in this manner when prompted.

If access to the local administration menu is not required on the enterprise network, i.e., if manual configuration is not done, or if it is only done in a controlled staging environment before IP Deskphones are deployed on the enterprise network, access to the menu can be completely disabled by setting the PROCSTAT parameter to 1 in the Settings File.

If access to the local administration menu is required on the enterprise network to protect against the unauthorized configuration of this interface, Avaya recommends that a customer-specific password for access be configured via Avaya Aura® Communication Manager for H.323 Deskphones (Figure 1) or via Session Manager/PPM (Figure 2) for SIP Deskphones. Knowledge of this password should remain highly confidential and rigorously controlled. Although this password may be alternately configured within the Settings File, this method is not recommended as the contents of the Settings File may be accessed, displayed and easily read using any web browser.

For further security, SNMP should be disabled by ensuring that the Community String is set to null. If it is enabled, access should be restricted by specifying one or more Source IP Address(es) used by the Network Management System. These values should also be configured via Avaya Aura Communication Manager for H.323 Deskphones (Figure 1) or via Session Manager/PPM (Figure 2) for SIP Deskphones.

To disallow physical access to the IP Deskphone serial console port when used with Avaya IP Office systems, update the Settings File to set PROCSTAT to value of 1, an action that completely disables the ability to manually administer IP Deskphone settings and consequently to enable physical access to the serial console port.

Remote Access

Remote access protocols such as Secure Shell (SSH) and Telnet were identified in the Study as a potential vulnerability for initiating attacks on other devices on customer networks. The following 96xx IP Deskphone models support Secure Shell (SSH) as means of secure remote access; 9608, 9611G, 9621G and 9641G. All other 96xx models as well as software for all 16xx and 46xx IP Deskphones do not support remote access. SSH, like the serial console port, is disabled by default and must be deliberately enabled to permit remote access of the device. To maintain the highest level of security, Avaya recommends that SSH remain disabled. In this way, a user must be present on the business premises and at the phone itself to enter the password using the dial pad of the target phone to enable this port to function as a console/debugging port.

In Summary:

IP telephone security vulnerabilities were identified in a Study and CVE. While Avaya 96xx, 16xx and 46xx IP Deskphones provide a serial console port connection which could be used to gain control over an IP telephone device, the following steps may be taken to deter such an attempt in Avaya 96xx, 16xx and 46xx IP Deskphones. For example:

- Avaya 96xx, 16xx and 46xx IP Desk Phones are provided by Avaya with the serial console port disabled. Make sure the serial console port remains disabled.
- Do not use the Settings file to change the password. Avaya Aura Communication Manager and Avaya Aura Session Manager may configure this password via a secure link to the IP Deskphone. SNMP should also be disabled or access restricted via this mechanism.
- Set the value of PROCSTAT to 1 for IP Office implementations, or for any installation where access to the local administration menu is not required on the enterprise network.
- Avaya 96x1 IP Deskphone running H323 6.2 or SIP 6.2 and later firmware releases are provided by Avaya with SSH disabled and consequently remote access to the device is disabled by default. Make sure SSH remains disabled on the Avaya IP Deskphone.
- Always upgrade the Avaya 96xx, 16xx and 46xx series Avaya IP Desk Phones firmware to the latest release.

Figure 1 Configure Phone Admin Password within Avaya Communication Manager

display system-parameters ip-options

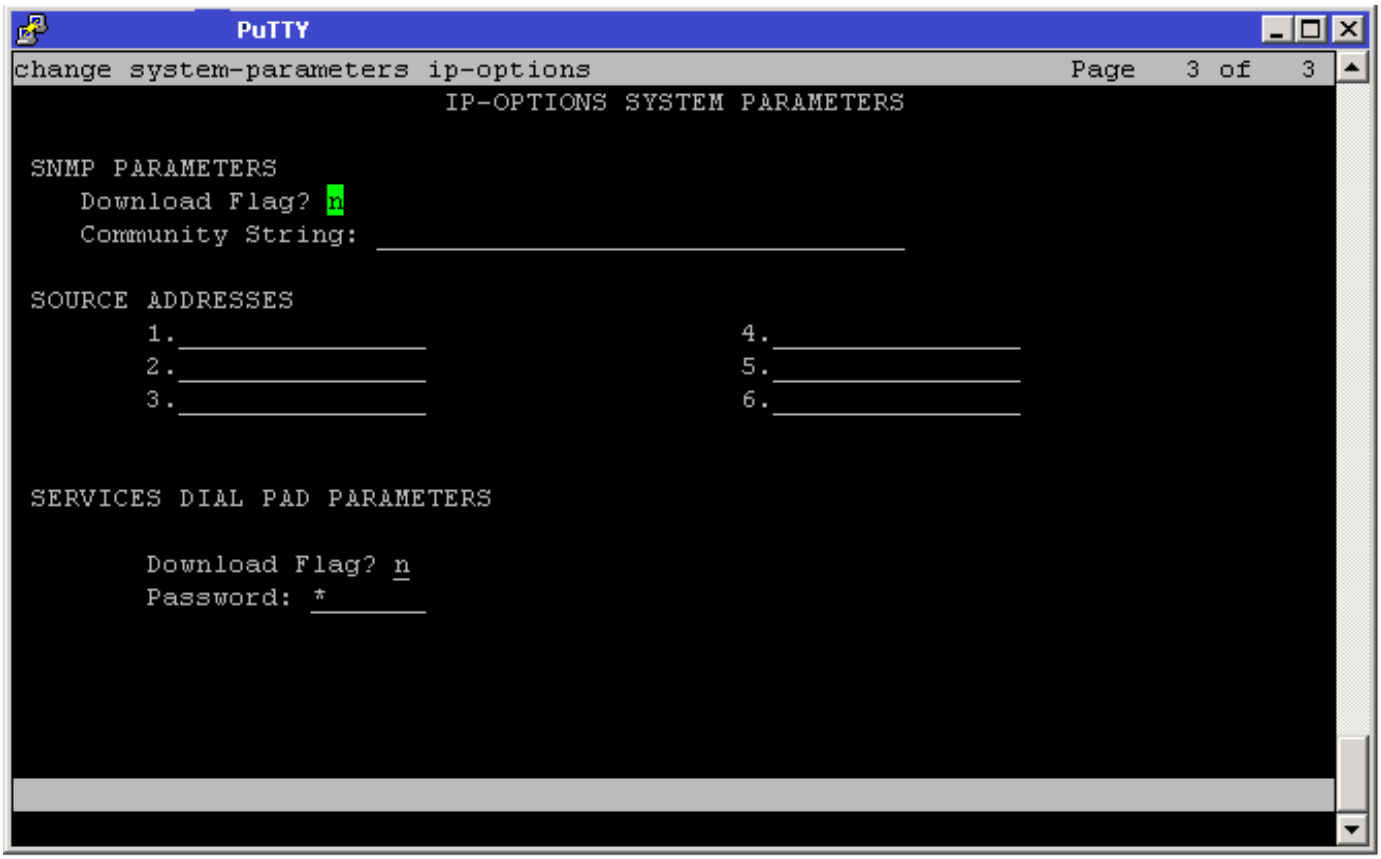
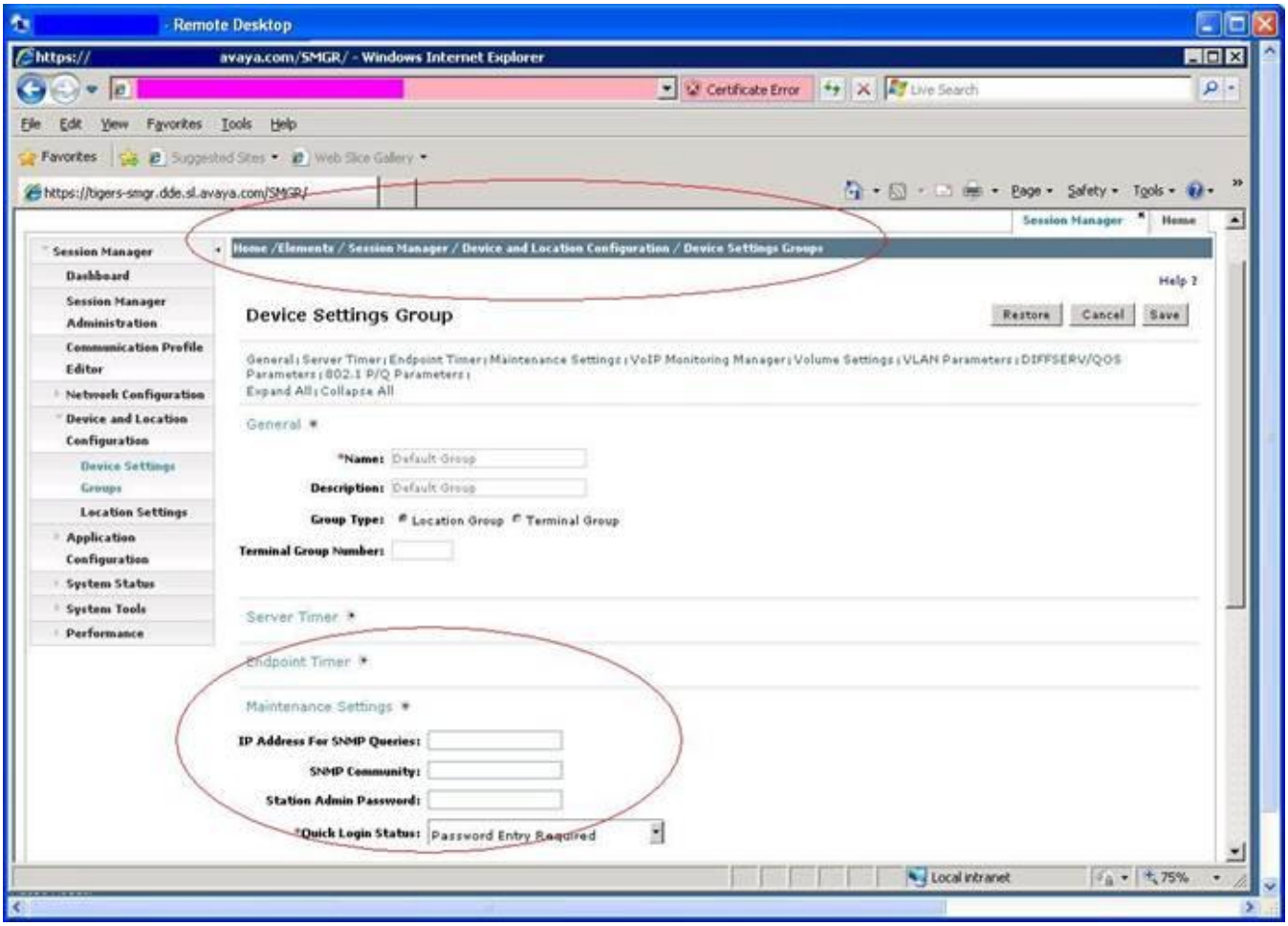


Figure 2 Configure Phone Admin Password within Avaya Session Manager

Home/Elements/Session Manager/Device and Location Configuration/Device Settings Groups



Resolution
n/a
Workaround or alternative remediation
n/a
Remarks
n/a

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch	
n/a	
Download	
n/a	
Patch install instructions	Service-interrupting?
n/a	No
Verification	
n/a	
Failure	
n/a	

Patch uninstall instructions

n/a

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

n/a

Avaya Security Vulnerability Classification

Not Susceptible

Mitigation

n/a

For additional support, contact your Authorized Service Provider. Depending on your coverage entitlements, additional support may incur charges. Support is provided per your warranty or service contract terms unless otherwise specified.

Avaya Support Contact	Telephone
U.S. Remote Technical Services – Enterprise	800-242-2121
U.S. Remote Technical Services – Small Medium Enterprise	800-628-2888
U.S. Remote Technical Services – BusinessPartners for Enterprise Product	877-295-0099
BusinessPartners for Small Medium Product	Please contact your distributor.
Canada	800-387-4268
Caribbean and Latin America	786-331-0860
Europe, Middle East, and Africa	36-1238-8334
Asia Pacific	65-6872-8686