Service Bulletin

Security Advisory

No. 20130206-0074 / Revised 06-Feb-2013

Overview

One of the primary advantages of the Allworx family of products is its flexibility in configuration and settings in a way that is easy to understand. Security is an important consideration, and we are constantly striving to improve our systems to protect our partners and their customers. It is also equally imperative that you never knowingly put your customer in a situation where it is easy for fraudulent attacks to compromise their Allworx systems.

We are investigating reported instances and have seen fraudulent SIP registration attacks that search public IP addresses and gain access to either an Allworx server or, most recently, to remote Allworx handsets not installed behind a firewall. We have also received reports of recent toll fraud incidents in which fraudulent attacks take over the SIP registration of an Allworx handset attached to a public network. This document summarizes the security best practices to prevent security compromises.

What You Should Do

When installing an Allworx system, it is imperative to use the proper security settings so that hostile, unauthorized attempts to access the system do not result in situations where either remote access or the spoofing of handsets can occur. Most often, the result is unauthorized calling and toll fraud. Compromises usually start with port scans to determine if a host is a candidate for unauthorized access. Disabling the use of ports often discourages a fraudulent attack, and the attacker will move on to another IP.

Please implement the following practices when installing any Allworx system:

Server

- Update every server to the most recent patch level of either the 7.3 or 7.4 software release. For example, releases 7.3.14.8 and higher, or 7.4.10.2 and higher. These patches change each Allworx phone SIP registration passwords during the phone reboot.
- Install the server behind a firewall or connect it to the public internet using the WAN port. **DO NOT** connect the Allworx LAN port directly onto the public internet.
- Disable Allworx WAN services (ports) not in use.
- Change voicemail ports (SMTP and IMAP) to non-standard port numbers.
- Change all server admin, phone admin, and user passwords from the default values.
- Use strong passwords for server and phone administration pages. **DO NOT** use simple passwords such as “1234” or “Allworx”.
- Verify that there is no exposure of the Admin Page (Port 8080) to the Public network. **DO NOT** port forward directly to the LAN port of an Allworx server from the customer’s router. For remote maintenance, use the Allworx VPN. Navigate to **Home** > **Network** > **VPN** > **modify** to configure the VPN settings.

When configuring WAN interface to connect to the public internet:

- Enable the server in NAT Firewall mode, preferably with Stealth DMZ. In stealth mode, the WAN interface does not respond to “pings” from other devices.

Remote phones

Password protection is very important to avoid fraudulent attacks on remote phones. Implement the following practices when installing an Allworx remote phone:

- Use a strong password for the phone administration password. **DO NOT** use simple passwords such as “1234” or “Allworx”, (**Home**>**Servers**>**VoIP** >**modify**> Phone Administration Password).
- Use a strong password for the Plug ’n’ Play Secret Key. **DO NOT** use simple passwords such as “1234” or “Allworx”. (**Home**>**Servers**>**VoIP** > **modify** > Plug ‘n’ Play Secret Key).
- Use proper firewall protection to connect remote Allworx phones to the public Internet. Allworx handsets provide web access to important information, including its login credentials and SIP Registration password. Phones with weak Phone Administration Passwords can easily have the SIP Registration passwords stolen.
- Disable Phone Creates via LAN and WAN Plug and Play except during phone installation.

Px Expander

- Change the Px admin password from the default value.
- Use a strong password for the Px admin password. **DO NOT** use a simple password such as “1234” or “Allworx”.
- Use proper firewall protection to connect remote Allworx Px Expanders to the public Internet. The Px Expander provides web access to important information, including its login credentials and SIP Registration password.
- Disable Phone Creates via LAN and WAN Plug and Play except during phone installation.

Other Considerations

Evidence from recent security incidents ***does not*** show attackers penetrating firewalls to access customer LANs or the servers/phones on customer LANs. Nonetheless, because aggressive malware/botnet/spyware attacks are known to compromise many desktop PCs, encourage customers to deploy LAN security solutions including:

- Maintaining up-to-date anti-virus/anti-malware protection on LAN systems.
- Deploying phones on VLANs to reduce opportunities to sniff SIP phone network traffic. This also improves network Quality of Service for phone traffic.
- Reporting any observed activity to Allworx Technical support immediately so we can investigate and stay in front of these malicious attempts.