Service Bulletin

Security Advisory

No. 20140415-Malformed-TCP / Revised 04-15-2014

Allworx Server Malformed TCP Option Denial of Service Vulnerability

Revision 1.0
Last Updated 2014 April 15
For Public Release 2014 April 15

Summary

Multiple versions of Allworx Server software releases are affected by a vulnerability when receiving a malformed TCP packet that triggers a problematic server response. This creates a network processing thread on the Allworx Server causing it to be unresponsive. Once this occurs, the only solution is to restart the system using the power button.

Summary of Related Incidents

Widespread incidents affecting Allworx servers circa April 7, 2014

- On April 7, 2014, Allworx servers in numerous locations became unresponsive. Data collected from some of the affected systems identified an Allworx Server software problem in handling certain malformed TCP packets.
- We are currently unable to identify the source of these malformed packets, and cannot predict whether another wave of server outages will occur in the future. By April 9, 2014, these incidents seem to have subsided (but could recur in the future).
- Allworx Support welcomes additional information from the field – in particular, packet captures around the time of systems becoming unexpectedly unresponsive. This information could help to understand what new attack tools might be leading this increase in a novel network probing activity.
- Tentative observations include the following:
  - It is possible that external firewalls or Server firewall rules, that limit TCP packets with unusual TCP options, may have limited the vulnerability of some sites. There is no

recommended external firewall configuration at this time; Allworx recommends installing patched server software to eliminate this vulnerability.

Affected Products

Vulnerable Products

The vulnerability is present in all Allworx Server software releases:

- Allworx Server prior to 7.4.19.2, 7.5.15.2, and 7.6.6.5
- All releases of 7.3 or earlier

Products Confirmed Not Vulnerable

- See “Software Versions and Fixes” below for patch release numbers that are not vulnerable.

Details

Impact

When a server becomes unresponsive due to this vulnerability, reboot the server as follows:

- Press the server power button for more than one second - but not more than 4 seconds. The server starts the shutdown process and the power light blinks green to confirm it is powering down. Allow sufficient time for the server to complete the power down cycle. Depending on the server, this process varies in length of time - from a few seconds to a few minutes. If the server has not properly shutdown after several minutes, hold the power button down for more than 5 seconds or unplug the AC power cord from the power outlet to force a shutdown. Caution: Rebooting the server this way may cause database corruption conditions causing further service disruption.
- Press the server power button for less than one second to start the server (pushing the power button for more than one second restarts the server in safe mode.) The server restarts and methodically starts the process to register the phones. The size of the system and number of handsets affects the duration of this process (possibly several minutes).

Software Versions and Fixes

- Allworx Server software versions 7.4.19.2, 7.5.15.2, and 7.6.6.5 are currently being tested by the Quality Assurance Team. We anticipate the fixes will be available on the Allworx Portal as early as April 18th and identified in the Release Notes as Defect # 16741.

Workarounds

The best preventative measure is to install software with a fix for this vulnerability.

Exploitation and Public Announcements

Allworx Support is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

Allworx Case IDs

Support case 101800

Development case 16741

Revision History

Revision 1.0	2014-April-15	Initial public release