Service Bulletin

Security Advisory

No. 20200312-0001/ Revised March 12, 2020

Allworx® Server products are vulnerable to an unauthorized data access exploit

Revision 1.0
Last Updated March 12, 2020
For Public Release March 12, 2020

Summary

Allworx servers running firmware version 8.0 and higher are vulnerable to an exploit that allows an actor to gain access to certain file data residing on the server without providing valid user credentials.

Affected Products

Vulnerable Products

- Allworx Servers

Products Not Vulnerable

- Allworx IP phones
- Allworx software applications
- Allworx portal

Additional Details

The exploit functions by initiating a download of certain temporary files that were previously generated through actions performed by a server administrator. One example of a temporary file in this category is a diagnostic log that is created using the **Tools > Advanced Troubleshooting > Advanced Diagnostic Logging** web page.

For the vulnerability to be exploited, several conditions must be met:

- A system administrator must have been logged into the server and created the file.
- The actor must have a properly-formed URL pointing to the file.

- The actor must be on the private network (LAN) or, if they are acting from the public network (WAN), port 8443 must be exposed in the server's firewall (i.e., NAT Firewall Mode) or forwarded from a security appliance (i.e., LAN Host Mode).

Recommended Next Steps

Sites that are concerned about this exposure should take the following actions as soon as possible:

- Disable HTTPS access (port 8443) to the server from the public network (Connect servers only).
- Delete any temporarily-created files on the server, such as diagnostics, etc. Server admins should get into a habit of immediately deleting these files after downloading them.
- Update the server to System Software version 8.4.14.9, 8.5.9.9, or 8.6.2.10 (or higher) as soon as possible.
- After the server and all phones have completed upgrading firmware, do the following:
  - Reboot all Allworx handsets from the server.
  - Create new passwords for all generic SIP handsets.
  - Change all SIP Proxy and SIP Gateway passwords.

Sites that have upgraded to the proper version of firmware may choose to re-enable port 8443 HTTPS access, however, it's **strongly recommended** that remote administration is done with either the Secure Remote Administration feature (via port 8043) or the VPN feature.

Secure Remote Administration enables a form of 2-factor authentication by using client-side certificates to authenticate devices; proper user credentials are still required. This feature is available on servers running System Software version 8.5 and higher.

The VPN feature is available on all Allworx System Software versions.

Please refer to the Allworx System Software Administrator Guide for details on how to configure and use these capabilities.

Sites concerned about these or other vulnerabilities should also:

- Regularly update the Allworx System Software to the most recent version available on the Allworx portal
- Procure and install SSL certificates on the Allworx Connect™ servers

Revision History

Revision 1.0	March 12, 2020	Initial public release