Grandstream Security Bulletin
GS20-GXW001 - Important

Security Vulnerability Associated with Unauthenticated Password Retrieval

Revision: 1.1

Published: Thursday, April 16, 2020
Updated: Monday, April 20, 2020

Summary

This security bulletin describes a vulnerability in the Grandstream GXW4501/4502/4504 series digital VoIP gateways that could allow malicious users to obtain user passwords.

Description

A recent security issue was discovered regarding SQL injections that could allow malicious unauthenticated users to retrieve the passwords of created users from the GXW4501/4502/4504 series digital VoIP gateways with firmware 1.0.0.32 or older. When certain actions are invoked on specific ports, the related modules will be vulnerable to the aforementioned SQL injections and brute force attacks.

Affected Models

The following models have been known to be affected by this issue:

- GXW4501
- GXW4502
- GXW4504

Affected Firmware

GXW4501/4502/4504 firmware 1.0.0.32 or older versions are affected.

* If your GXW4501/4502/4504 is on a test build or a Beta firmware, it is most likely affected as well.

Solution/Recommendation:

GXW4501/4502/4504 firmware 1.0.0.35 has patched this security vulnerability. Grandstream strongly recommends all GXW4501/4502/4504 to be upgraded to the current official firmware 1.0.0.35 **IMMEDIATELY**.

After upgrading, please make sure to change web access passwords for ALL users in GXW450x web UI->Maintenance->User Management page, which includes super admin and admin users. It's also highly recommended to change the username to be different from the previous username. If any unknown user exists in User Management page, please remove it immediately.

Support

To obtain help and support for this security update:

- Explore and use the Grandstream Forums at http://forums.grandstream.com
- Submit a technical support ticket at https://helpdesk.grandstream.com/
- Read the UCM Security Manual, which can be downloaded from:
  http://www.grandstream.com/sites/default/files/Resources/UCM_Security_Manual.pdf