Grandstream Security Bulletin GS13-UCM002 – Important

Potential Vulnerability Associated With Misuse of Dial Trunk Option in IVR

Published: Tuesday, August 06, 2013

Version: 1.0

General Information

Summary

This security bulletin describes a potential vulnerability in the Grandstream UCM6100 series IP PBX appliances which may allow unauthorized calls when user optionally enables the "Dial Trunk" configuration parameter without setting up proper outbound route permissions as reported in the Grandstream forum and some other Internet forums.

Description

Grandstream received reports indicating the UCM6100 series IP PBX appliances may allow incoming calls into the IVR with the "Dial Trunk" option enabled to dial unauthorized toll calls using trunks and outbound routes configured on the UCM6100.

The "Dial Trunk" option in UCM6100 is designed to allow IVR callers to be able to reach extensions in a remote peer PBX. For better flexibility we offer a "Permission" setting that would be applied to calls out of the IVR, regardless of the original caller's granted privilege.

When calls are made from within IVR that needs to be routed via an outbound route using trunks, the UCM6100 will compare the IVR "Permission" setting with the Outbound Route's "Privilege Level" setting. Such calls will be rejected if the IVR "Permission" is lower than the Outbound Route's "Privilege Level." For more details on permissions and privilege levels, please consult this document.

There are two scenarios unauthorized toll calls via trunks might possibly happen when the IVR "Dial Trunk" option is enabled:

1. The IVR "Permission" setting is set at the default "Internal" level (default); and there exists outbound routes allowing toll calls with "Privilege Level" set at "Internal" (default).
2. The IVR "Permission" setting is set higher than the default and

minimal “Internal” level; and there exists outbound routes allowing toll calls with “Privilege Level” set at a level equal or lower than the IVR “Permission.”

Recommendation/Solution. Please check your UCM6100’s configuration for all Outbound Routes and make sure each one of them have the appropriate “Privilege Level” configured. **Grandstream strongly recommends using one of the Local, National, or International settings for any route that would incur tolls.**

It is also strongly recommended that users keep the IVR “Permission” setting at the default “Internal” level, and enable “Dial Trunk” option only if necessary.

Grandstream plans to add the DISA (Direct Inward System Access) application to the UCM6100 soon. The IVR “Dial Trunk” and “Permission” settings will be obsolete once the DISA application is added.

Please consult the Grandstream’s FAQ or support system if you have questions on how to configure IVR to fit your need.

Affected Models

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

UCM6102
UCM6104
UCM6108
UCM6116

Support

How to obtain help and support for this security update

- Using Grandstream Forum at http://forums.grandstream.com
- Submit a technical support ticket at http://www.grandstream.com/support/submit-a-ticket

Disclaimer