# Grandstream Security Bulletin GS19-UCM004 – Important

## Security Vulnerability Associated With Unauthorized Call via SIP Trunk

Published: Monday, December 16, 2019, Dec 16 Version: 1.0

### Summary

This security bulletin describes a potential vulnerability in the Grandstream UCM6100/6200/6510 series IP PBX appliances which could allow malicious users to make unauthorized outbound/toll calls via existing SIP trunk on the UCM.

### Description

Grandstream received reports indicating that on the UCM6100/6200/6510 series IP PBX appliances 1.0.19.27 or older firmware version, unauthorized outbound/toll calls can be made by remote users when manipulating certain "From:" domain using the SIP trunk on the UCM. The UCM admin may notice undesired calls from CDR on UCM webUI later on if call activity is not closely monitored.

The reason for this vulnerability is related to the internal matching rule that allows endpoint user with certain "From:" domain to use existing SIP trunk to dial out from the trunk, especially when outbound route is not strictly defined.

### Affected Models

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

- UCM6102
- UCM6104
- UCM6108
- UCM6116
- UCM6202
- UCM6204
- UCM6208
- UCM6510

### Affected Firmware

1.0.19.27 or lower versions are affected.

* If your UCM is on a test build or a Beta Test firmware, it is most likely affected as well.

## Solution/Recommendation:

New UCM firmware 1.0.19.29 for UCM62xx/6510 and 1.0.18.17 has added the fix to prevent this security vulnerability. The internal matching rule that allows user with certain "From:" domain to dial out via trunk is removed.

It's also recommended for UCM admin to avoid configuring outbound route with simple rules such as "xxxx". A more strict and specific rule should be used to prevent unauthorized outbound calls to be successfully made.

**Grandstream strongly recommends all UCM62xx/6510 to be upgraded to 1.0.19.27 IMMEDIATELY, and all UCM61xx to be upgraded to 1.0.18.17 IMMEDIATELY.**

## Support

How to obtain help and support for this security update:

Use Grandstream Forum at http://forums.grandstream.com

Submit a technical support ticket at https://helpdesk.grandstream.com/

UCM Security Manual can be downloaded from:
http://www.grandstream.com/sites/default/files/Resources/UCM_Security_Manual.pdf

## Disclaimer

Asterisk, AsteriskGUI, and AsteriskNOW are registered trademarks of Digium, Inc.