Grandstream Security Bulletin GS17-UCM003 – Important

Security Vulnerability Associated With Returned Cookie from WebUI Login Session

Published: Monday, Oct 02, 2017 Version: 1.0

Updated: Thursday, Jan 11, 2017 Version: 1.2

Summary

This security bulletin describes a potential vulnerability in the Grandstream UCM6100/6200/6510 series IP PBX appliances which could allow malicious users to send out a CGI requests without actually logging in to the web UI to operate the UCM.

Description

Grandstream received reports indicating that on the UCM6100/6200/6510 series IP PBX appliances 1.0.14.23 or older firmware version, the web UI shows a suspicious unrecognized admin user being created. This malicious admin user then logs in to the UCM and performs a series of operations such as downloading extension file, changing inbound/outbound routes, deleting CDR and etc. Unauthorized toll calls can be made after the UCM data and configuration have been compromised. Furthermore, the system administrator might not be able to notice these unauthorized toll calls right away because the malicious admin user deletes CDR after making calls.

The reason for this vulnerability is related to cookie “session-identify” being set in the CGI login request after a legitimate successful login and then the cookie is returned to the web browser upon a failed login attempt.

Affected Models

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

- UCM6102
- UCM6104
- UCM6108
- UCM6116
- UCM6202
- UCM6204

- UCM6208
- UCM6510

Affected Firmware

1.0.14.23 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 has added the following fix to prevent this security vulnerability:

1. Added fix on cookie return behavior, in the case that the UCM login password is wrong, no cookie session-identify will be returned. This fix is added on firmware 1.0.14.24 and 1.0.15.14+. Future firmware will also include the fix.
2. On UCM web UI->System Settings->HTTP Server page, option "Enable IP Address Whitelist" is supported and up to 10 permitted IPs can be added. Once "Enable IP Address Whitelist" is enabled, only the permitted IP can visit UCM web UI page. This feature is added in firmware 1.0.15.14+. Future firmware will also include it.

NOTE:

1. **If your UCM is still on 1.0.14.23 or older version, please review UCM web UI sections "Operation Log" and "User Management" under Maintenance page for any suspicious user creation and activity. If any unauthorized users are found, please remove them immediately. Please make sure there is no unauthorized user created for login and then upgrade to 1.0.14.24 or 1.0.15.14+ immediately.**
2. **Grandstream strongly recommends all UCMs to be upgraded to 1.0.14.24 or 1.0.15.14+ 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