Grandstream Security Bulletin
GS20-HT8XX001 - Important

Revision: 1.0

Published: August 03, 2020

Summary

This security bulletin describes a vulnerability in the Grandstream HT8XX ATAs that could allow malicious users to obtain device information, crash the device, get into root shell, or put TR-069 services into infinite loop or crash the service. Solutions and guidelines are also provided with details.

Description

Grandstream received reports indicating that on the HT80X/HT812/HT814/HT818 series ATAs 1.0.17.5 or older firmware versions and on HT813 1.0.5.2 or older firmware versions, unauthorized command injection can be made during device provision, certain TCP messages could trigger infinite loop in TR-069, unauthenticated remote HTTP Get request may crash the TR-069 services and root shell is accessible via SSH.

Affected Models

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

- HT801
- HT802
- HT812
- HT814
- HT818
- HT813

Affected Firmware

For HT80X/HT812/HT814/HT818, firmware 1.0.17.5 or lower versions are affected.

For HT813, firmware 1.0.5.2 or lower versions are affected.

* If your HT8XX is on a test build or a Beta firmware, it is most likely affected as well.

Solution/Recommendation:

HT80X/HT812/HT814/HT818 firmware 1.0.19.11 and HT813 1.0.7.1 has patched these security vulnerabilities.

Grandstream strongly recommends all HT80X/HT812/HT814/HT818 to be upgraded to 1.0.19.11 IMMEDIATELY, and all HT813 to be upgraded to 1.0.7.1 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/

HT8XX Security Manual can be downloaded from:
http://www.grandstream.com/sites/default/files/Resources/HT8xx_Security_Manual.pdf