MWR LABS

Security Advisory

Amazon Echo Rooting

19/07/2017

Hardware	Amazon Echo
Affected Models	2015, 2016
CVE Reference	N/A
Author	Mark Barnes
Severity	Medium
Vendor	Amazon
Vendor Response	Fixed

Description:

The Amazon Echo is an ‘always listening’ smart speaker utilising Amazons Alexa Amazon Voice Services (AVS).

The device was found to be vulnerable to a physical attack that allows an attacker to gain root access to the underlying Linux operating system.

Impact:

An attacker with physical access could deliver malware onto the device which would grant them persistent remote access and the ability to stream live microphone without altering the functionality of the device or leaving physical evidence of tampering.

Such a vulnerability raises a number of privacy concerns about 'always listening' devices which is important to customers and their trust relations with Amazon.

Cause:

This vulnerability is due to two hardware design choices of the Amazon Echo:

- Exposed debug pads on the base of the device
- Hardware configuration that allows for the device to be booted from an external SD Card

The exposed debug pads are easily accessible on the base of the Amazon Echo exposing both UART and connections for an external SD Card. The hardware is configured such that the device will attempt to boot first from this exposed SD Card before the internal memory.

Solution:

The SD Card pads on the 2017 edition of the Amazon Echo have been disabled preventing the device from being booted externally.

As this is a hardware fix 2015 and 2016 devices will remain vulnerable.

Vendor Response and Recommendation:

“Customer trust is very important to us. To help ensure the latest safeguards are in place, as a general rule, we recommend customers purchase Amazon devices from Amazon or a trusted retailer and that they keep their software up-to-date.” - Amazon

Technical details

Prior researchers were able to boot into a generic Linux environment from an external SD Card attached to debug pads on the base of an Amazon Echo. They made their processes, details of the debug pins, and a bootable SD Card image available on their public Github wiki [1], they also published a white paper [2] which further speculated on how to root the Echo.

We connected an SD Card with a bootable image to the Amazon Echo and monitored the UART port. During a cold restart we interrupted the boot process and entered into the U-Boot bootloader command line interface. From there it was possible to inspect the content of the file systems on the internal memory, chose which Kernel and root file system to load and change the Linux boot parameters. Through examination of the partitions on the internal memory we identified the location of the primary Linux kernel and root files system for the device. We changed U-Boot environment variables to boot from this partition and modify the Linux boot parameters such that the file system is mounted with read/write access (normally it mounts as read only) and runs '/bin/sh' on initialisation.

On our test device these variables can be set using the following U-Boot commands:

```
uboot> setenv mmc_part 1:7
uboot> setenv root /dev/mmcblk0p7
uboot> setenv mmcargs 'setenv bootargs console=${console} root=${root} ${mount_type}
rootfstype=ext3 rootwait ${config_extra} init=/bin/sh'
uboot> setenv mount_type rw
```

Once booted a root terminal is presented over UART bypassing any authentication. At this stage no initialisation scripts have been ran and the watchdog daemon is not running causing the device to reboot after a few seconds.

To spawn a watchdog daemon we ran the following command:

```
sh-3.2# /usr/local/bin/watchdogd
```

The environment is now stable however none of the main services have been started and the device is not fully functional. However we do have full read/write access to the entire file system which can modify as root.

Further technical details can be found in our blog post [3].

1. https://github.com/echohacking/wiki/wiki/Echo
2. https://vanderpot.com/Clinton_Cook_Paper.pdf
3. https://labs.mwrinfosecurity.com/blog/alexa-are-you-listening

Detailed Timeline

Date	Summary
15-05-2017	Issue reported to Amazon Security
15-05-2017	Amazon Security responded with confirmation of the issue
15-07-2017	MWR queried Amazon Security on the issue status
17-07-2017	MWR found that new devices were not vulnerable
24-07-2017	Amazon Lab126 Security contacted MWR to discuss the vulnerability and release date
01-08-2017	Public disclosure of vulnerability and technical blog post