Samsung Smart TV Wi-Fi Direct Improper Authentication

1. Advisory Information

Title: Samsung Smart TV Wi-Fi Direct Improper Authentication
Advisory ID: NESESO-2017-0313
Advisory URL: http://neseso.com/advisories/NESESO-2017-0313.pdf
Date published: 2017-04-19
Date of last update: 2017-03-13
Vendors contacted: Samsung
Release mode: User Release

2. Vulnerability Information

Class: Improper Authentication [CWE-287]
Impact: Security bypass
Remotely Exploitable: Yes
Locally Exploitable: No

3. Vulnerability Description

Samsung Smart TVs running Tizen OS are prone to a security vulnerability that allows an attacker to impersonate a trusted device to obtain unrestricted access without authentication when connected via Wi-Fi Direct[1].

4. Vulnerable Packages

- UN32J5500 Firmware version 1480

Other products and versions might be affected too, but they were not tested.

5. Vendor Information, Solutions and Workarounds

Neseso recommends to remove all the whitelisted devices and avoid using the WiFi-Direct feature.

Contact the vendor for further information.

6. Credits

This vulnerability was discovered and researched by a member from Neseso Research Team.

7. Technical Description

Wi-Fi Direct Improper Authentication

Wi-Fi Direct [1], initially called Wi-Fi P2P, is a Wi-Fi standard enabling devices to easily connect with each other without requiring a wireless access point. It is useful for everything from internet browsing to file transfer, and to communicate with one or more devices simultaneously at typical Wi-Fi speeds. In a scenario where two devices want to connect they can authenticate using methods such as PIN, Push-Button or NFC.

Samsung TVs has support for Wi-Fi Direct by default and it's enabled every time the device it's turn on. The system uses a blacklist/whitelist access control mechanism to avoid asking the user to authenticate devices every time they try to connect using WiFi-Direct. This access control mechanism uses the MAC address to identify the devices, making easy for an attacker to get the necessary information to impersonate a whitelisted device and gain access to the Smart TV. The user will get notified about the whitelisted device connecting to the Smart TV, but no authentication it's required. Once connected the attacker have access to all the services provided by the TV, such as remote control service or DNLA screen mirroring. If any of the services provided by the Smart TV, once connected using WiFi-Direct, is vulnerable the attacker could gain control of the Smart TV or use it to pivot and gain access to the network where the Smart TV is connected to.

8. Report Timeline

- 2017-03-13: Neseso attempted to contact Samsung security contact.
- 2017-03-17: Neseso attempted to contact Samsung security contact for second time.
- 2017-03-20: Samsung replied that it's possible to use the BugBounty site.
- 2017-03-20: Neseso reply asking for a public key to communicate in a secure manner.
- 2017-03-20: Samsung send their public key.
- 2017-03-21: Neseso sent the advisory document.
- 2017-03-22: Samsung replied they were looking into the issue.
- 2017-03-27: Neseso asks the vendor if they were able to verify the vulnerability.
- 2017-03-28: Samsung Smart TV Bug Bounty Team replied they need an attack scenario and explanation about how to reproduce the vulnerability. They also sent their public key.
- 2017-03-28: Neseso requests a public key that it's not expired.
- 2017-03-28: Neseso found a valid public key on the vendor web site and sent the attack scenario description and how to reproduce the vulnerability.
- 2017-03-30: Neseso asks the vendor if they were able to verify the vulnerability.
- 2017-03-31: Samsung replied they just started issue analysis.
- 2017-04-06: Samsung replied they concluded that this is not a security threat to Samsung TV.

9. References

[1] - http://www.samsung.com/in/support/skp/faq/441202

10. About Neseso

Neseso is an independent security consulting company with more than 10 years of experience in security research and vulnerability assessment.

11. Copyright Notice

The contents of this advisory are copyright (c) 2016 Neseso and are licensed under a Creative Commons Attribution Non-Commercial Share-Alike 4.0 License: http://creativecommons.org/licenses/by-nc-sa/4.0/