TLP: WHITE

MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2017-033

DATE(S) ISSUED:
04/05/2017

SUBJECT:
A Vulnerability in Apple iOS Could Allow for Arbitrary Code Execution

OVERVIEW:
A vulnerability has been discovered in Apple iOS, which could allow for arbitrary code execution. This vulnerability can be exploited by anyone within Wi-Fi range of the affected device. Successful exploitation of this vulnerability could result in arbitrary code execution within the context of the Wi-Fi chip. Depending on the privileges associated with the Wi-Fi chip, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If the Wi-Fi chip has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:
- iOS 10 versions prior to 10.3

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in Apple iOS, which could allow for arbitrary code execution. This vulnerability can be exploited by anyone within Wi-Fi range of the affected device. Continuous sending of specially crafted wireless frames can cause an overflow of the firmware stack, allowing for a buffer overflow to occur. (CVE-2017-6975)

Successful exploitation of this vulnerability could result in arbitrary code execution within the context of the Wi-Fi chip. Depending on the privileges associated with the Wi-Fi

chip, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If the Wi-Fi chip has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Apply appropriate patches provided by Apple to vulnerable systems immediately after appropriate testing.

REFERENCES:
Apple:
https://support.apple.com/en-us/HT207688

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6975

24×7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722