Critical Vulnerability Affecting Billions of Devices Identified Thanks to Moabi.Com

San Francisco, Mar 27, 2020 (Issuewire.com**)** - Moabi, the pioneer in IoT Firmware Security, shared the results of an in-depth analysis of the popular Hostapd software performed using its revolutionary online SaaS platform. Those results have been made public at the San Francisco RSA 2020 conference:

https://www.rsaconference.com/usa/agenda/automotiveiot-network-exploits-from-static-analysis-to-reliable-exploits

Hostapd is used in billions of devices to enable wifi access point functionality. During an audit of the GenIVI Alliance software, it appeared that Hostapd is vulnerable to multiple cryptographic vulnerabilities due to the improper seeding of Pseudo-Random Number Generators (PRNGs), potentially leading to remote compromise of wifi networks. Those vulnerabilities have been assigned numbers CVE-2016-10743 and CVE-2019-10064.

Hostapd (host access point daemon) is a user-space daemon software enabling a network interface card to act as an access point and authentication server. It is powering billions of IoT devices.

It has been discovered that hostapd before version 2.6 wasn't seeding PRNGs at all. This vulnerability has been fixed silently around 2016, but never attributed a CVE number, leading to many distributions and IoT devices still shipping this version of

the software. This vulnerability has been given id CVE-2016-10743.

In some configurations, when WPS is enabled and a /dev/urandom device isn't available, this leads to WPS PINS being predictable, allowing remote network access from an attacker.

In addition, it has been discovered that the Extensible Authentication Protocol (EAP) model, which offers protection against flooding attacks, also uses predictable PRNGs. This vulnerability has been assigned id CVE-2019-10064.

In order to protect themselves from those vulnerabilities, users should upgrade their versions of Hostapd to the latest available patchset.

A complete technical advisory is available here: https://moabi.com/advisories/CVE-2019-10064.html

About Moabi:

Moabi SaaS platform is an award-winning pro-active security solution to audit software, firmware, binaries and their dependencies. Learn more about Moabi at https://moabi.com

Media Contact

Moabi

arnaud.gardin@moabi.com

+33 687 687 450

Source : Moabi

See on IssueWire