Sierra Wireless Security Advisory CVE-2017-9247: Unquoted Service Path Vulnerabilities

Release Date: July 12, 2017

Issue Description:

Sierra Wireless has confirmed an issue with its Windows Mobile Broadband Driver Packages (MBDP) that could allow a malicious actor to potentially escalate privileges locally by inserting an executable on a service path used by the modem driver. The specific issue identified was that the driver package used an unquoted service path containing at least one whitespace character. There are two affected service paths:

1. The execution path for SwiService.exe. An executable placed on this service path would launch whenever the SwiService.exe was loaded.
2. The uninstall service path for MBDP. An executable placed on this service path would launch whenever the MBDP was uninstalled or upgraded.

These vulnerabilities are present on Sierra Wireless MBDP with build ID < 4657.

Impact:

A local authenticated attacker may be able to escalate privileges.

Solution:

Users should upgrade to the latest Sierra Wireless drivers. The upgrade process will patch the service paths before upgrade to avoid triggering any latent executables. Users which need to stay on the current version of driver can apply a patch to their registry entries. Please contact your device manufacturer for more information on the appropriate upgrade or patch for your platform.

Credits:

This issue was discovered by Alexandro Calò of Horizon Security (www.horizonsecurity.it).