

Product Security Advisory SWI-PSA-2020-002: Arbitrary Files Write Using Hard Link Vulnerability


Release Date: April 14, 2020

Description:

Sierra Wireless has confirmed a vulnerability with its Windows Mobile Broadband Driver Packages (MBDP) that could allow an unprivileged user to overwrite arbitrary files in arbitrary folders using hard links. CVE-2020-8948 has been assigned to this vulnerability.

The vulnerability is present on Sierra Wireless Mobile Broadband Driver Packages before Build 5043 for the following modules: EM7565, EM7511, EM7411, EM7455, MC7455, EM7430, MC7430, EM7355, MC7355, MC7354, EM7305, MC7305, MC7304, EM7330, MC7330, EM8805, MC8805.

To determine if your installation is affected, go to “Programs and Features” under the Windows Control Panel on your device and look for an entry for “Sierra Wireless Mobile Broadband Driver Package”. The build number is highlighted in yellow in the example below:

| | | | | |
|---|-----------------------|-----------|--------|----------------|
|  Sierra Wireless Mobile Broadband Driver Package | Sierra Wireless, Inc. | 7/27/2018 | 781 MB | 9.11.4838.0005 |
|---|-----------------------|-----------|--------|----------------|

Impact:

An unprivileged user can execute arbitrary code with SYSTEM privileges.

Solution:

Sierra Wireless advises users to upgrade to the latest version of MBDP for your product(s) and ensure you are running with build number \geq 5043. Contact your PC supplier for assistance if necessary.

Credits:

This vulnerability was discovered by Mads Joensen & Simon van Beest of Danish Cyber Defence and was published in the blog post [CVE-2020-8948: Local privilege escalation in Sierra Wireless EM7455](#). For further information please visit www.danishcyberdefence.dk.