PRODUCT SECURITY ADVISORY

NOVEMBER 1, 2021

PSIRT Record Number
CARR-PSA-002-1121

Overview

Hills ComNav is a remote access integration module for the Hills Reliance security alarm system. It allows you to easily access your security alarm system via telephone or internet anywhere in the world. Ever worry that you forgot to turn on your security system. Now with Hills ComNav you can easily phone your security system to check its status and remotely turn it on or off.

Multiple vulnerabilities have been discovered affecting the ComNav module.

1. No brute force protection for local login (CWE-307)
2. Unencrypted communication (CWE-311)
3. Predictable message size (CWE-342)
4. Weak encryption (CWE-326)

Impact

1. This vulnerability has a CVSS 3.1 score of 5.5 (Medium), with a vector string of CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N.

Last Update 11/01/2021 ©2021 Carrier. All Rights Reserved.

2. This vulnerability has a CVSS 3.1 score of 5.5 (Medium), with a vector string of CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N.
3. This vulnerability has a CVSS 3.1 score of 4.0 (Medium), with a vector string of CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
4. This vulnerability has a CVSS 3.1 score of 6.2 (Medium), with a vector string of CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N.

Affected Versions

The vulnerabilities effect all versions of ComNav up to and including 3002-19.

Solution

Carrier is offering free upgrades to version 4000-12 to mitigate these known vulnerabilities. The only way to accomplish this is to return your unit. Contact your installer for more details. Return postage to Carrier/Hills, and any on-premise labor including programming or configuration costs, are not included.

Mitigation

We strongly recommend changing the ComNav's default credentials, as well as PIN codes (i.e., from the defaults to longer 6-digit PIN codes).

Initial Publication Date	Last Published Date
November 1, 2021	November 1, 2021

Last Update 11/01/2021 ©2021 Carrier. All Rights Reserved.