# FragAttacks Hirschmann BAT

Date: 2022-08-01
Version: 1.1
References: CVE-2020-24586, CVE-2020-24587, CVE-2020-24588, CVE-2020-26142, CVE-2020-26144, CVE-2020-26145, CVE-2020-26146 and CVE-2020-26147[1]

## Executive Summary

FragAttacks[2] (fragmentation and aggregation attacks) is a collection of security vulnerabilities that affect Wi-Fi devices.

## Details

An adversary that is within range of a victim's Wi-Fi network can exploit these vulnerabilities to steal user information or attack devices.

The CVSS score of the vulnerabilities is rated as:

- CVE-2020-24586: Low CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:L/I:N/A
- CVE-2020-24587: Low CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
- CVE-2020-24588: Low: CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
- CVE-2020-26142: Medium: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N
- CVE-2020-26144: Medium: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
- CVE-2020-26145: Medium: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
- CVE-2020-26146: Medium: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N
- CVE-2020-26147: Medium: CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:H/A:N

## Impact

An attacker could use the vulnerability to compromise the availability of the device and/or gather user information.

## Affected Products

| Brand | Product Line / Platform | Product | Version | Scope |
|---|---|---|---|---|
| Hirschmann | HiLCOS | OpenBAT, WLC, BAT450 | All versions of 9.1x and lower<br>10.12-REL<br>10.12-RU1<br>10.12-RU2<br>10.12-RU3<br>10.12-RU4<br>10.12-RU5 | CVE-2020-24588<br>CVE-2020-26144<br>CVE-2020-26146<br>CVE-2020-26147 |
| Hirschmann | BAT-C2 | BAT-C2 | 08.08.01.00R08 or lower | CVE-2020-24586<br>CVE-2020-24587<br>CVE-2020-24588<br>CVE-2020-26142<br>CVE-2020-26144<br>CVE-2020-26145<br>CVE-2020-26146<br>CVE-2020-26147 |

## Solution

Updates are available, which address the vulnerability. Customers are advised to update their product.

| Brand | Product Line / Platform | Product | Version |
|---|---|---|---|
| Hirschmann | HiLCOS | OpenBAT, WLC, BAT450 | 10.12-RU6<br>10.12-RU7 |
| Hirschmann | BAT-C2 | BAT-C2 | 09.12.01.00R01 or higher |

## For Help or Feedback

To view all Belden Security Bulletins or to report suspected security vulnerabilities, go to https://www.belden.com/security.
For technical support and other requests, please visit https://hirschmann-support.belden.com.

## Related Links

- [1] https://nvd.nist.gov/vuln/detail/CVE-2020-24586
  https://nvd.nist.gov/vuln/detail/CVE-2020-24587
  https://nvd.nist.gov/vuln/detail/CVE-2020-24588
  https://nvd.nist.gov/vuln/detail/CVE-2020-26142
  https://nvd.nist.gov/vuln/detail/CVE-2020-26144
  https://nvd.nist.gov/vuln/detail/CVE-2020-26145
  https://nvd.nist.gov/vuln/detail/CVE-2020-26146
  https://nvd.nist.gov/vuln/detail/CVE-2020-26147

- [2] https://www.fragattacks.com/

## Disclaimer



## Revisions

V1.0 (2022-03-14): Bulletin published.
V1.1 (2022-08-01): Updated bulletin for Hirschmann BAT-C2 product.