Drägerwerk AG & Co.KGaA, 23542 Lübeck

Our reference
PSA-21-246-1

Vulnerability and Incident Reporting
product-security@draeger.com

**Dräger Product Security Advisory PSA-21-246-1**

FragAttacks Wi-Fi Vulnerabilities

**Legal Notice**

This Product Security Advisory is based on all our findings that we had at the time of publication. However, the facts of the case are being reviewed on an ongoing basis and it is possible that this may result in changed assessments or that assessments contained in this advisory may turn out to be incorrect. We also reserve the right to change or revoke any recommendations. In addition, differences may result from the circumstances of the individual case on site. This information is naturally not available to us and has not been taken into account. Dräger can therefore accept no responsibility that the information presented here is conclusive or comprehensively correct for you. Therefore, please check carefully to what extent deviations can arise for your individual case. If necessary, you will be informed about new findings through following advisories.

## 1 Publication Date

2021-09-03

## 2 Overview

In May 2021, the same researcher who discovered the KRACK vulnerabilities disclosed several new 802.11 vulnerabilities that affect nearly all known Wi-Fi devices, including clients and APs. In addition to the coordinated disclosure, a tool was released that can be used to test both clients and APs for the presence of these issues. There are two types of vulnerabilities here: fundamental design flaws in 802.11 that have been in the standard since 1997 and implementation defects that can vary by Wi-Fi vendor & product. All Draeger products tested (including M300, M540, and Delta) are vulnerable to one or more of these disclosed vulnerabilities.

The full text of this advisory can be accessed through https://static.draeger.com/security.

## 3 Affected Products

| ***Product*** | ***Status*** |
|---|---|
| ***Infinity® M300*** *(Hardware Revision <0.4)* | *Used Chipset: NXP Semiconductors BGW211* |
| ***Infinity® M300*** *(Hardware Revision ≥0.4)* | *Used Chipset: Redpine Signals RS9113* |
| ***Infinity® M540*** *(older Hardware Revisions)* | *Used Chipset: NXP Semiconductors BGW211* |
| ***Infinity® M540*** *(latest Hardware Revisions)* | *Used Chipset: Redpine Signals RS9113* |
| ***Infinity® Delta Series*** *(all Hardware Revisions)* | *Used Chipset: Ambicom Wireless Card* |
| ***Vista 120 S*** | *Used Chipset: Redpine Signals RS9113* |

## 4 How to verify if the product is affected

All devices listed under section 3 are affected.

## 5 Vulnerability Description

FragAttacks is a collection of vulnerabilities that affect many Wi-Fi devices.

From the author's website (https://www.fragattacks.com/):

> *The discovered vulnerabilities affect all modern security protocols of Wi-Fi, including the latest WPA3 specification. Even the original security protocol of Wi-Fi, called WEP, is affected. This means that several of the newly discovered design flaws have been part of Wi-Fi since its release in 1997! Fortunately, the design flaws are hard to abuse because doing so requires user interaction or is only possible when using uncommon network settings. As a result, in practice the biggest concern are the programming mistakes in Wi-Fi products since several of them are trivial to exploit.*

## 6 Impact

There are numerous vulnerabilities related to the FragAttacks. Dräger tested two versions of M540, two versions of M300, and one version of Delta. Different vulnerabilities affected each product, yet all products were affected by at least one vulnerability tested. Results are shown in the table below.

| | | Product Vulnerability Indicated By Test | | | | | |
|---|---|---|---|---|---|---|---|
| CVE | Description | M540 HW1.1 | M540 HW2.0 | M300 0.3HW | M300 0.4/0.5HW | Delta | Notes |
| **Design Flaws** | | | | | | | |
| CVE-2020-24588 | Accepting non-SPP A-MSDU frames | | ✓ | | ✓ | | |
| CVE-2020-24587 | Reassembling fragments encrypted under different keys | ✓ | ✓ | ✓ | ✓ | | |
| CVE-2020-24586 | Not clearing fragments from memory when (re)connecting to a network | ✓ | ✓ | ✓ | ✓ | ✓ | |
| **Implementation flaws allowing trivial packet injection** | | | | | | | |
| CVE-2020-26145 | Accepting plaintext broadcast fragments as full frames (in an encrypted network) | | | | | ✓ | |
| CVE-2020-26144 | Accepting plaintext A-MSDU frames that start with an RFC1042 header with EtherType EAPOL (in an encrypted network) | | ✓ | | ✓ | | |
| CVE-2020-26140 | Accepting plaintext data frames in a protected network | | ✓ | | ✓ | ✓ | |
| CVE-2020-26143 | Accepting *fragmented* plaintext data frames in a protected network | | ✓ | | ✓ | | |
| **Other Implementation Vulnerabilities** | | | | | | | |
| CVE-2020-26139 | Forwarding EAPOL frames even though the sender is not yet authenticated | | | | | | AP Only |
| CVE-2020-26146 | Reassembling encrypted fragments with non-consecutive packet numbers | ✓ | ✓ | ✓ | ✓ | ✓ | |
| CVE-2020-26147 | Reassembling mixed encrypted/plaintext fragments | ✓ | ✓ | ✓ | ✓ | | |
| CVE-2020-26142 | Processing fragmented frames as full frames | | | | | | |
| CVE-2020-26141 | Not verifying the TKIP MIC of fragmented frames | | N/A | | N/A | | TKIP not supported with BGW211 or Delta & not recommended for other platforms |

*Results of Dräger testing on M540, M300, and Delta devices.*

While Dräger only performed proof-of-concept testing on the versions listed above, the author of the FragAttacks vulnerabilities stated that every Wi-Fi product is affected by at least one FragAttack vulnerability.

From the author's website (https://www.fragattacks.com/):

> *…FragAttacks (fragmentation and aggregation attacks) which is a collection of new security vulnerabilities that affect Wi-Fi devices. An adversary that is within range of a victim's Wi-Fi network can abuse these vulnerabilities to steal user information or attack devices. Three of the discovered vulnerabilities are design flaws in the Wi-Fi standard and therefore affect most devices. On top of this, several other vulnerabilities were discovered that are caused by widespread programming mistakes in Wi-Fi products. Experiments indicate that every Wi-Fi product is affected by at least one vulnerability and that most products are affected by several vulnerabilities.*

Although Vista 120 was not tested, Vista 120 is affected. The hardware manufacturers will not replace the affected chipsets for any of the Dräger products listed in section 3. Therefore, all Dräger products listed in section 3 are affected and will continue to be affected.

## 7 Severity

21 vulnerabilities related to FragAttacks – see below for CVSS ranges

CVSS 3.1 Scores

Base Score: 1.8 – 4.8

Severity: Low – Medium

Vector: Varies by vulnerability

For the full list of CVEs, please visit https://www.fragattacks.com/ and view section “Assigned CVE Identifiers”.

## 8 Remediation

Due to the high sophistication and close proximity needed to carry out an attack, and the low value of the information an attacker would be able to decrypt, we estimate the risk of a successful attack against the possibly affected devices as improbable. Nevertheless, to further reduce the risk of PHI to be leaked, we suggest to refrain from using the patient name fields. To reduce the risk of forged messages introduced on the Wi-Fi channel, we suggest to configure the network to use AES-CCMP encryption.

## 9 Contact Information

If you have any further questions related to the impact of the vulnerabilities, please contact your designated regional marketing manager. For reporting incidents and potential vulnerabilities in our devices, please refer to https://static.draeger.com/security to contact the Product Security team directly.

## 10 Revision History

| VERSION | DATE | COMMENTS |
|---|---|---|
| 1.0 | 2021-09-03 | Initial Advisory |

Drägerwerk AG & Co. KGaA
Moislinger Allee 53-55
23558 Lübeck, Germany
Postal address:
23542 Lübeck, Germany
Tel +49 451 882-0
Fax +49 451 882-2080
info@draeger.com
www.draeger.com
VAT no. DE135082211

Bank details:
Commerzbank AG, Lübeck
IBAN: DE95 2304 0022 0014 6795 00
Swift-Code: COBA DE FF 230
Sparkasse zu Lübeck
IBAN: DE15 2305 0101 0001 0711 17
Swift-Code: NOLADE21SPL

Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7903 HL
General partner: Drägerwerk Verwaltungs AG
Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7395 HL

Chairman of the Supervisory Board
for Drägerwerk AG & Co. KGaA
and Drägerwerk Verwaltungs AG:
Stefan Lauer
Executive Board:
Stefan Dräger (chairman)
Rainer Klug
Gert-Hartwig Lescow
Dr. Reiner Piske
Anton Schrofner