REVISION: A
DATE: 2021-08-05
DOC. NUMBER: 9AKK107992A4463

HITACHI ABB

CYBERSECURITY ADVISORY

FragAttacks Vulnerabilities in Hitachi ABB Power Grids TropOS Product

CVE-2020-24586
CVE-2020-24587
CVE-2020-24588
CVE-2020-26139
CVE-2020-26140
CVE-2020-26141
CVE-2020-26142
CVE-2020-26143
CVE-2020-26144
CVE-2020-26145
CVE-2020-26146
CVE-2020-26147

Notice

Affected Products and Versions

The followings are the affected products and product versions:

- All 4th generation TropOS products including 1420, 2420 and 6420 with TropOS Firmware v8.9.4.8 and earlier versions.

Summary

Hitachi ABB Power Grids is aware of public reports of the FragAttacks vulnerability in the product versions listed above.

An attacker could use a weakness in the Wi-Fi protocol to implement a man-in-the-middle attack, snooping Wi-Fi frames and appending undetected packet fragments that could be used spoof IP address and/or DNS information. A client connected to a TropOS Wi-Fi access point could directed to fake websites, used to extract sensitive data.

Note that the TropOS mesh traffic is not vulnerable. TropOS nodes are also not affected. However, a TropOS mesh or device could be used to transport modified Wi-Fi/IP frames.

Vulnerability ID, Severity and Details

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

CVE ID	Detail Description
CVE-2020-24586 fragment cache attack (not clearing fragments from memory when (re)connecting to a network) CVSS v3.1 Base Score: 3.5 Low CVSS v3.1 Vector: /AV:A/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N Link to NVD: click here	The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that received fragments be cleared from memory after (re)connecting to a network. Under the right circumstances, when another device sends fragmented frames encrypted using WEP, CCMP, or GCMP, this can be abused to inject arbitrary network packets and/or exfiltrate user data.
CVE-2020-24587 mixed key attack (reassembling fragments encrypted under different keys) CVSS v3.1 Base Score: 2.6 Low CVSS v3.1 Vector: /AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N Link to NVD: click here	The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that all fragments of a frame are encrypted under the same key. An adversary can abuse this to decrypt selected fragments when another device sends fragmented frames and the WEP, CCMP, or GCMP encryption key is periodically renewed.
CVE-2020-24588 aggregation attack (accepting non-SPP A-MSDU frames) CVSS v3.1 Base Score: 3.5 Low CVSS v3.1 Vector: /AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N Link to NVD: click here	The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that the A-MSDU flag in the plaintext QoS header field is authenticated. Against devices that support receiving non-SSP A-MSDU frames (which is mandatory as part of 802.11n), an adversary can abuse this to inject arbitrary network packets.

CVE-2020-26139 Forwarding EAPOL frames even though the sender is not yet authenticated (should only affect APs). CVSS v3.1 Base Score: 5.3 Medium CVSS v3.1 Vector: /AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H Link to NVD: click here	An Access Point (AP) forwards EAPOL frames to other clients even though the sender has not yet successfully authenticated to the AP. This might be abused in projected Wi-Fi networks to launch denial-of-service attacks against connected clients and makes it easier to exploit other vulnerabilities in connected clients.
CVE-2020-26140 Accepting plaintext data frames in a protected network. CVSS v3.1 Base Score: 6.5 Medium CVSS v3.1 Vector: /AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N Link to NVD: click here	The WEP, WPA, WPA2, and WPA3 implementations accept plaintext frames in a protected Wi-Fi network. An adversary can abuse this to inject arbitrary data frames independent of the network configuration.
CVE-2020-26141 Not verifying the TKIP MIC of fragmented frames. CVSS v3.1 Base Score: 6.5 Medium CVSS v3.1 Vector: /AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N Link to NVD: click here	The Wi-Fi implementation does not verify the Message Integrity Check (authenticity) of fragmented TKIP frames. An adversary can abuse this to inject and possibly decrypt packets in WPA or WPA2 networks that support the TKIP data-confidentiality protocol.
CVE-2020-26142 Processing fragmented frames as full frames. CVSS v3.1 Base Score: 7.5 High CVSS v3.1 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N Link to NVD: click here	The WEP, WPA, WPA2, and WPA3 implementations treat fragmented frames as full frames. An adversary can abuse this to inject arbitrary network packets, independent of the network configuration.
CVE-2020-26143 Accepting fragmented plaintext data frames in a protected network. CVSS v3.1 Base Score: 6.5 Medium CVSS v3.1 Vector: /AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N Link to NVD: click here	The WEP, WPA, WPA2, and WPA3 implementations accept fragmented plaintext frames in a protected Wi-Fi network. An adversary can abuse this to inject arbitrary data frames independent of the network configuration.
CVE-2020-26144 Accepting plaintext A-MSDU frames that start with an RFC1042 header with EtherType EAPOL (in an encrypted network). CVSS v3.1 Base Score: 6.5 Medium CVSS v3.1 Vector: /AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N Link to NVD: click here	The WEP, WPA, WPA2, and WPA3 implementations accept plaintext A-MSDU frames as long as the first 8 bytes correspond to a valid RFC1042 (i.e., LLC/SNAP) header for EAPOL. An adversary can abuse this to inject arbitrary network packets independent of the network configuration.
CVE-2020-26145 Accepting plaintext broadcast fragments as full frames (in an encrypted network). CVSS v3.1 Base Score: 6.5 Medium CVSS v3.1 Vector: AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N Link to NVD: click here	The WEP, WPA, WPA2, and WPA3 implementations accept second (or subsequent) broadcast fragments even when sent in plaintext and process them as full unfragmented frames. An adversary can abuse this to inject arbitrary network packets independent of the network configuration.
CVE-2020-26146 Reassembling encrypted fragments with non-consecutive packet numbers. CVSS v3.1 Base Score: 5.3 Medium CVSS v3.1 Vector: /AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N Link to NVD: click here	The WPA, WPA2, and WPA3 implementations reassemble fragments with non-consecutive packet numbers. An adversary can abuse this to exfiltrate selected fragments. This vulnerability is exploitable when another device sends fragmented frames and the WEP, CCMP, or GCMP data-confidentiality protocol is used. Note that WEP is vulnerable to this attack by design.

CVE-2020-26147 Reassembling mixed encrypted/plaintext fragments. CVSS v3.1 Base Score: 5.4 Medium CVSS v3.1 Vector: /AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:H/A:N Link to NVD: click here	The WEP, WPA, WPA2, and WPA3 implementations reassemble fragments even though some of them were sent in plaintext. This vulnerability can be abused to inject packets and/or exfiltrate selected fragments when another device sends fragmented frames and the WEP, CCMP, or GCMP data-confidentiality protocol is used.

Vulnerability Details

A full detailed description of the Wi-Fi fragmentation vulnerabilities including a number of helpful videos, can be found at https://www.fragattacks.com/ [1]. We suggest carefully reading the exploitability statement as described in the finder's report [1].

Recommended Immediate Actions

The problem is corrected in the following future product versions:

Affected Version	Corrected Version
TropOS Firmware v8.9.4.8 and earlier versions	TropOS Firmware v8.9.4.9

Hitachi ABB Power Grids recommends that customers apply the update at the earliest convenience.

Mitigation Factors/Workarounds

Hitachi ABB Power Grids has tested and recommends the following mitigation actions:

- Disable the Wi-Fi access on any TropOS unit where local Wi-Fi access is not required. This is achieved by NOT enabling (or disabling) the local access SSID.
- Where Wi-Fi access is required, wherever possible ensure that physical access to the local area is restricted to approved staff only.
- Use the Wi-Fi whitelist capability to restrict Wi-Fi access to only approved personnel.
- As the FragAttacks vulnerability is targeted at an end-user device and generally involves redirection to fraudulent websites, the installation of comprehensive firewall capabilities on company end-user devices and servers will significantly reduce the likelihood of negative outcomes.

Although these mitigation strategies will not remediate the underlying vulnerability, they can help block known attack vectors.

Frequently Asked Questions

What is the scope of the vulnerability?

A complex to exploit vulnerability that presents a remote possibility of a Wi-Fi end-user being redirected to unsecure websites.

What causes the vulnerability?

This vulnerability leverages an incomplete Wi-Fi packet fragmentation/reassembly validation. In theory, a bad actor could capture Wi-Fi packets and appended invalid packet fragments that misdirects user IP traffic.

What might an attacker use the vulnerability to do?

The main risk is the redirection of an end-user to an insecure, fake website that is used to extract personal and/or financial information such as credit card numbers.

How could an attacker exploit the vulnerability?

The main risk is the redirection of an end-user to an insecure, fake website that is used to extract personal and/or financial information such as credit card numbers.

Could the vulnerability be exploited remotely?

The attacker has to be physically close to the TropOS access point and end-user device. The vulnerability requires the capture and replay of Wi-Fi packets with invalid, appended data.

What does the update do?

The update adds complete validation of fragmented packets. When data is appended to packets, the sanity check fails, and the packet is discarded.

When this security advisory was issued, had this vulnerability been publicly disclosed?

Yes, the FragAttacks vulnerability has been publicly disclosed [1].

When this security advisory was issued, had Hitachi ABB Power Grids received any report that this vulnerability was being exploited?

There is no indication that this vulnerability has been exploited on a TropOS network.

References

1. FragAttacks, https://www.fragattacks.com/

Support

For additional information and support please contact your product provider or Hitachi ABB Power Grids service organization. For contact information, see https://www.hitachiabb-powergrids.com/contact-us/ for Hitachi ABB Power Grids contact-centers.