AFS Series – HSR Denial-of-Service Vulnerability

CVE-2020-9307

Notice

Affected Products and versions

AFS660/AFS665 including following variants: • AFS660-SR • AFS665-SR	Version 7.0.07 (HSR Firmware variant) *Previous versions are not affected*

Vulnerability ID

CVE ID: CVE-2020-9307

Summary

A crafted HSR frame can cause a denial of service on one of the ports in an HSR ring.

Vulnerability Severity

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.

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:N/A:H

CVSS v3.1 Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H&version=3.1

NVD Summary Link: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9307

Vulnerability Details

A change in the HSR implementation of the AFS660/AFS665 Version 07.0.07 introduced a vulnerability. It could allow an unauthenticated, adjacent attacker to cause a denial-of-service on one of the HSR ring ports of the device.

Recommended immediate actions

Customers are advised to update their AFS660/AFS665 product to HSR firmware Version 7.1.03. Hitachi ABB Power Grids recommends that customers apply the update at the earliest convenience. Please contact your local support.

Mitigation Factors

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

Workarounds

There are no workarounds available.

Frequently Asked Questions

What is the scope of the vulnerability?

A successful attack on a device in an HSR ring causes one of the ports in the ring to no longer switch packets, effectively breaking the redundancy of the HSR ring. If the attacker can perform the same attack on a second device, the ring is broken into two parts, thus disrupting communication between devices in the different parts.

What is the affected product or component?

AFS660/AFS665 which are running HSR firmware with version from 7.0.07

What does the update do?

The update removes the vulnerability by modifying the way that the switch processes HSR frames

What causes the vulnerability?

A change in the HSR implementation of the AFS660/AFS665 Version 7.0.07 introduced a vulnerability

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted HSR frame. An attacker must be inside the network to launch the attack.

Could the vulnerability be exploited remotely?

No, to exploit this vulnerability an attacker would need to have physical access to an affected system node.

What does the update do?

The update removes the vulnerability by modifying the way that the switch processes HSR frames

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

Yes, this vulnerability has been publicly disclosed.

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

No, Hitachi ABB Power Grids had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued

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.