TLP:CLEAR
REVISION: 1
PUBLICATION DATE: 2023-05-25
DOC. IDENTIFIER: 8DBD000149
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Multiple libexpat vulnerabilities in Hitachi Energy's AFS65x, AFS67x, AFR67x and AFF66x series Products

CVE-2022-40674
CVE-2022-43680

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of multiple vulnerabilities in the open source “libexpat” that affects the AFS65x, AFS66x, AFS67x, AFR67x and AFF66x series Products versions listed below. Please refer to the Recommended Immediate Actions for information about the mitigation or remediation.
Successful exploitation of this vulnerability could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS).

Vulnerability ID, Severity and Details

The vulnerability’s severity assessment is performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1. The CVSS Environmental Score, which can affect the final vulnerability severity score, is not provided in this advisory as it reflects the potential impact of the vulnerability in the customer organizations’ computing environment. Customers are recommended to analyze the impact of the vulnerability in their environment and calculate the CVSS Environmental Score.

Vulnerability ID	Detail Description
CVE-2022-40674 CVSS v3.1 Base Score: 9.8 Critical CVSS v3.1 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Link to NVD: click here	libexpat library is incorporated in our AFS, AFR and AFF products family. libexpat before 2.4.9 has a use-after-free in the doContent function in xmlparse.c. Successful exploitation of this vulnerability could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS).
CVE-2022-43680 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:N/A:H Link to NVD: click here	libexpat library is incorporated in our AFS, AFR and AFF products family. In libexpat through 2.4.9, there is a use-after free caused by overeager destruction of a shared DTD in XML_ExternalEntityParserCreate in out-of-memory situations. Successful exploitation of this vulnerability could lead to Denial of Service (DoS).

Recommended Immediate Actions

The Table below shows the affected version and the recommended immediate actions.

Affected Version	Recommended Actions
AFS660/665S, AFS660/665C, AFS670v2 Firmware 7.1.05 and earlier	Apply mitigation strategy as described in General Mitigation Factors Section or update to upcoming 7.1.08 when available.
AFS670/675, AFR67x Firmware 9.1.07 and earlier	Apply mitigation strategy as described in General Mitigation Factors Section or update to 9.1.08.
AFS65x	EoL product - only mitigation available, no remediation expected. Apply mitigation strategy as described in General Mitigation Factors Section.
AFF660/665 Firmware 03.0.02 and earlier	Apply mitigation strategy as described in General Mitigation Factors Section or update to upcoming release.

Hitachi Energy recommends that customers apply the update at the earliest convenience.

General Mitigation Factors

In addition, recommended security practices and firewall configurations can help protect a process control network from attacks that originate from outside the network. Such practices include that process control systems are physically protected from direct access by unauthorized personnel, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed, and others that have to be evaluated case by case. Process control systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system.

Frequently Asked Questions

What are the affected products, AFx series products?

AFx series products cover a broad range of optical networks communication solutions for industrial networks.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited these vulnerabilities could disclose sensitive information, addition or modification of data, or Denial of Service (DoS).

How could an attacker exploit the vulnerability?

An attacker could exploit the vulnerabilities by creating a specially formed HTTP requests and sending the message to an affected device. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit these vulnerabilities. Recommended practices include that process control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

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

No, these vulnerabilities have not yet been publicly disclosed.

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

No, Hitachi Energy had not received any information indicating that these vulnerabilities had been exploited when this security advisory was originally issued.

Support

This advisory will be updated as new relevant information becomes available. Please subscribe to Hitachi Energy's Cybersecurity Alerts & Notifications to get notified:

https://www.hitachienergy.com/offering/solutions/cybersecurity/alerts-and-notifications/subscribe

For additional information and support please contact your product provider or Hitachi Energy service organization. For contact information, see https://www.hitachienergy.com/contact-us/ for Hitachi Energy contact-centers.

Publisher

Hitachi Energy PSIRT – cybersecurity@hitachienergy.com

Revision

Date of the Revision	Revision	Description
2023-04-25	1	Initial public release.

DocuSigned by: