REVISION: B
PUBLICATION DATE: 2021-12-02
DOC. IDENTIFIER: 8DBD000057
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Multiple Open-Source Software Related Vulnerabilities in Hitachi Energy Transformer Asset Performance Management (APM) Edge

CVE-2017-8872
CVE-2019-1547
CVE-2019-1549
CVE-2019-1563
CVE-2019-20388
CVE-2020-1971
CVE-2020-10713
CVE-2020-14308
CVE-2020-14309
CVE-2020-14310
CVE-2020-14311
CVE-2020-15705
CVE-2020-15706
CVE-2020-15707
CVE-2020-14372
CVE-2020-24977
CVE-2020-25632
CVE-2020-27749
CVE-2020-27779
CVE-2021-3449
CVE-2021-3516
CVE-2021-3517
CVE-2021-3518
CVE-2021-3537
CVE-2021-3541
CVE-2021-20225
CVE-2021-20233
CVE-2021-23840
CVE-2021-23841

Notice

The information in this document is subject to change without notice and should not be construed as a commitment by Hitachi Energy. Hitachi Energy provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall Hitachi Energy or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if Hitachi Energy or its suppliers have been advised of the possibility of such damages. This document and parts hereof must not be reproduced or copied without written permission from Hitachi Energy and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose. All rights to registrations and trademarks reside with their respective owners.

Summary

Hitachi Energy is aware of public reports of the vulnerabilities in the followings open-source software, namely OpenSSL, LibSSL, libxml2 and GRUB2 bootloader. Some of the vulnerabilities affect the Transformer Asset Performance Management (APM) Edge product versions listed below.

An attacker who successfully exploited this vulnerability could cause the product to become inaccessible.

An update that resolves the vulnerabilities is available.

Affected Products and Versions

List of affected products and product versions:

– APM Edge Version 1.0

– APM Edge Version 2.0

– APM Edge Version 3.0

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.

OpenSSL, LibSSL Components

CVE-ID	Severity, Vector and Link to NVD
CVE-2021-3449	CVSS v3.1 Base Score: 5.9 Medium CVSS v3.1 Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H Link to NVD: click here
CVE-2020-1971	CVSS v3.1 Base Score: 5.9 Medium CVSS v3.1 Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H Link to NVD: click here
CVE-2019-1563	CVSS v3.0 Base Score: 3.7 Low CVSS v3.0 Vector: /AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H Link to NVD: click here
CVE-2019-1549	CVSS v3.0 Base Score: 5.3 Medium CVSS v3.0 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Link to NVD: click here
CVE-2019-1547	CVSS v3.0 Base Score: 4.7 Medium CVSS v3.0 Vector: /AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N Link to NVD: click here

CVE-2021-23840	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
CVE-2021-23841	CVSS v3.0 Base Score: 5.9 Medium CVSS v3.0 Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H Link to NVD: click here

LibXML2

CVE-ID	Severity, Vector and Link to NVD
CVE-2017-8872	CVSS v3.1 Base Score: 9.1 Critical CVSS v3.1 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H Link to NVD: click here
CVE-2019-20388	CVSS v3.0 Base Score: 7.5 High CVSS v3.0 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Link to NVD: click here
CVE-2020-24977	CVSS v3.0 Base Score: 6.5 Medium CVSS v3.0 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L Link to NVD: click here
CVE-2021-3516	CVSS v3.0 Base Score: 7.8 High CVSS v3.0 Vector: /AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H Link to NVD: click here
CVE-2021-3517	CVSS v3.0 Base Score: 8.6 High CVSS v3.0 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H Link to NVD: click here
CVE-2021-3518	CVSS v3.0 Base Score: 8.8 High CVSS v3.0 Vector: /AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H Link to NVD: click here
CVE-2021-3537	CVSS v3.0 Base Score: 5.9 Medium CVSS v3.0 Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H Link to NVD: click here
CVE-2021-3541	CVSS v3.0 Base Score: 6.5 Medium CVSS v3.0 Vector: /AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H Link to NVD: click here

GRUB2

CVE-ID	Severity, Vector and Link to NVD
CVE-2020-10713	CVSS v3.0 Base Score: 8.2 High CVSS v3.0 Vector: /AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H Link to NVD: click here

CVE-2020-14308	CVSS v3.0 Base Score: 6.4 Medium CVSS v3.0 Vector: /AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H Link to NVD: click here
CVE-2020-14309	CVSS v3.0 Base Score: 6.7 Medium CVSS v3.0 Vector: /AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H Link to NVD: click here
CVE-2020-14310	CVSS v3.0 Base Score: 6.0 Medium CVSS v3.0 Vector: /AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H Link to NVD: click here
CVE-2020-14311	CVSS v3.0 Base Score: 6.0 Medium CVSS v3.0 Vector: /AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H Link to NVD: click here
CVE-2020-15705	CVSS v3.0 Base Score: 6.4 Medium CVSS v3.0 Vector: /AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H Link to NVD: click here
CVE-2020-15706	CVSS v3.0 Base Score: 6.4 Medium CVSS v3.0 Vector: /AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H Link to NVD: click here
CVE-2020-15707	CVSS v3.0 Base Score: 6.4 Medium CVSS v3.0 Vector: /AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H Link to NVD: click here
CVE-2020-14372	CVSS v3.0 Base Score: 7.5 High CVSS v3.0 Vector: /AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H Link to NVD: click here
CVE-2020-25632	CVSS v3.0 Base Score: 8.2 High CVSS v3.0 Vector: /AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H Link to NVD: click here
CVE-2020-27749	CVSS v3.0 Base Score: 6.7 Medium CVSS v3.0 Vector: /AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H Link to NVD: click here
CVE-2020-27779	CVSS v3.0 Base Score: 7.5 High CVSS v3.0 Vector: /AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H Link to NVD: click here
CVE-2021-20225	CVSS v3.0 Base Score: 6.7 Medium CVSS v3.0 Vector: /AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H Link to NVD: click here
CVE-2021-20233	CVSS v3.0 Base Score: 8.2 High CVSS v3.0 Vector: /AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H Link to NVD: click here

The following lists the following possible impact of those vulnerabilities:

– **Encryption key recovery:** An attacker with access to the network can exploit the vulnerabilities related to OpenSSL and LibSSL components resulting in a possibility to recover the transported encryption key or decrypt any RSA encrypted message that was encrypted with the public RSA key.

– **Memory information retrieval and possible application crash:** An attacker with access to the network can exploit the vulnerabilities related to LibXML2 and may retrieve information from the memory. This type of attack may also cause the application to crash causing denial-of-service.

– **GRUB2 UEFI Secure Boot Bypass:** It was discovered that GRUB2 contained various vulnerabilities that would allow Unified Extensible Firmware Interface (UEFI) Secure Boot to be bypassed. A local attacker with administrative privileges (or with physical access to the system) could use this issue to circumvent GRUB2 module signature checking, resulting in the ability to load arbitrary GRUB2 modules that have not been signed by a trusted authority and hence bypass UEFI Secure Boot.

Recommended Immediate Actions

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

Affected Version	Recommended Actions
Transformer APM Edge v1.0, v2.0, v3.0	Update to Transformer APM Edge v4.0

Whenever applicable, Hitachi Energy recommends that customers apply the update at the earliest convenience. The update updates the software components where the vulnerabilities are remediated.

Mitigation Factors/Workarounds

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 is APM Edge Product?

Transformer APM Edge is an on-premises Transformer Asset Performance Management product. Trans-former APM Edge collects input data from various sensors, sensor aggregator solutions and then provides the user a display of all of the health/status of all transformers. The product is used for monitoring purpose only.

What is the scope of the vulnerability?

There are four main scope for the vulnerabilities described in this advisory:

- Application crash causing an application denial of service.
- Encryption key recovery.

- Memory information retrieval.
- Secure boot bypass.

The vulnerability may cause the Transformer APM Edge to crash and consequently, the monitoring function of the transformer fleet would be suspended until the APM Edge is back online.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause the affected system node application to stop or become inaccessible.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability. 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?

Yes, these vulnerabilities have been publicly disclosed by the respective Open-Source Software teams.

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 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 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
2021-11-02	A	Initial public release.
2021-12-02	B	Update title page – removed irrelevant CVE-IDs