REVISION: B
PUBLICATION DATE: 2021-12-23
DOC. IDENTIFIER: 8DBD000079
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

OWASP Related Vulnerabilities in Hitachi Energy's LinkOne Product

CVE-2021-40337
CVE-2021-40338
CVE-2021-40339
CVE-2021-40340

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of private report of OWASP[1] related vulnerabilities in the Hitachi Energy LinkOne product versions listed below. An update is available that resolves the reported vulnerabilities.

An attacker who successfully exploited these vulnerabilities could modify victim's system files or information, disclose application full path, disclose sensitive information to unauthorized actor, and launch common web attack.

Affected Products and Versions

List of affected products and product versions:

– LinkOne WebView v3.20

– LinkOne WebView v3.22

– LinkOne WebView v3.23

– LinkOne WebView v3.24

– LinkOne WebView v3.25

– LinkOne WebView v3.26

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-2021-40337 CVSS v3.1 Base Score: 4.2 Medium CVSS v3.1 Vector: AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N Link to NVD: click here CWE-79 : Cross Site Scripting	Multiple Stored XSS vulnerability exists in the LinkOne application. An attacker that manages to exploit the vulnerability can take advantage to exploit multiple web attacks and stole sensitive information.
CVE-2021-40338 CVSS v3.1 Base Score: 3.7 Low CVSS v3.1 Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N Link to NVD: click here CWE-309 : Generation of Error Message Containing Sensitive Information	When an error happens during the query operation in the application, due to a misconfiguration in the web server configuration file, debug mode in LinkOne application is activated and showing full path of the directory.

[1] OWASP : Open Web Application Security Project®

CVE-2021-40339 CVSS v3.1 Base Score: 3.7 Low CVSS v3.1 Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N Link to NVD: click here CWE-16 : Configuration	The LinkOne application is lacking HTTP Headers. An attacker that manages to exploit this vulnerability may retrieve sensitive information.
CVE-2021-40340 CVSS v3.1 Base Score: 3.7 Low CVSS v3.1 Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N Link to NVD: click here CWE-200 : Exposure of Sensitive Information to an Unauthorized Actor	Misconfiguration in the ASP server causes server and ASP.net information to be shown. An attacker can use this information as a reconnaissance for further exploitation.

Recommended Immediate Actions

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

Affected Version	Recommended Actions
LinkOne WebView v3.20	Apply security patch or update to LinkOne v3.27
LinkOne WebVIew v3.22	Apply security patch or update to LinkOne v3.27
LinkOne WebView v3.23	Apply security patch or update to LinkOne v3.27
LinkOne WebVIew v3.24	Apply security patch or update to LinkOne v3.27
LinkOne WebView v3.25	Apply security patch or update to LinkOne v3.27
LinkOne WebVIew v3.26	Apply security patch or update to LinkOne v3.27

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

General Mitigation Factors/Workarounds

Recommended security practices and firewall configurations can help protect the application from attacks that originate from outside the network. Such practices include that the application is physically protected from direct access by unauthorized personnel, have no direct connections to the Internet. For the end-user of the application, it is recommended to use the latest browser when accessing the LinkOne application.

Additional recommendation is to follow the hardening guidelines published by “The Center for Internet Security (CIS)” https://www.cisecurity.org/about-us/ to protect the host Operating System on which the LinkOne is hosted.

Frequently Asked Questions

What is Hitachi Energy LinkOne product?

LinkOne is an enterprise graphical parts catalog and content delivery solution for publishing, viewing and finding information for complex equipment and assemblies.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited these vulnerabilities could exploit multiple web attacks and retrieve sensitive information.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerabilities by accessing the LinkOne application and insert a script instead of normal input.

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 application 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, Hitachi Energy received information about this vulnerability through responsible disclosure.

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.

Acknowledgement

Hitachi Energy thanks the following for working with us to help protect our customers:

Compañía Minera Doña Inés de Collahuasi SCM.

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
2021-12-22	A	Initial public release.
2021-12-23	B	Updated the Recommended Actions with security patch availability info.