CYBERSECURITY ADVISORY

Cross Site Request Forgery (CSRF) and HTTP Response Splitting in Hitachi Energy’s MSM Product
CVE-2021-40335
CVE-2021-40336

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 an internal report of multiple vulnerabilities in the MSM versions listed below. Please refer to the Recommended Immediate Actions for recommended mitigation actions.
An attacker who successfully exploit this vulnerability, could trick the user into downloading malicious software onto his computer instead of accessing the MSM web interface.

Affected Products and Versions
List of affected products and product versions:
- MSM version 2.2 and earlier.

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.

<table>
<thead>
<tr>
<th>Vulnerability ID</th>
<th>Detail Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2021-40335</td>
<td>A vulnerability exists in the HTTP web interface where the web interface does not sufficiently verify if a well-formed, valid, consistent request was intentionally provided by the user who submitted the request. This cause a Cross Site Request Forgery (CSRF), which if exploited could lead an attacker to gain unauthorized access to the web application and perform an unwanted operation on it without the knowledge of the legitimate user. An attacker who successfully makes an MSM user who has already established a session to MSM web interface clicks a forged link to the MSM web interface, e.g., link is sent per E-Mail, could perform harmful command on MSM through its web server interface.</td>
</tr>
<tr>
<td>CVE-2021-40336</td>
<td>A vulnerability exists in the http web interface where the web interface does not validate data in an HTTP header. This causes a possible HTTP response splitting, which if exploited could lead an attacker to channel down harmful code into the user’s web browser such as to steal the session cookies. Thus, attacker who successfully makes an MSM user who has already established a session to MSM web interface clicks a forged link to the MSM web interface, e.g., link is sent per E-Mail, could trick the user into downloading malicious software onto his computer.</td>
</tr>
</tbody>
</table>
Recommended Immediate Actions

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

<table>
<thead>
<tr>
<th>Affected Version</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSM version 2.2 and earlier</td>
<td>Apply mitigation strategy as described in Mitigation Factors Section.</td>
</tr>
</tbody>
</table>

Mitigation Factors

Recommended security practices and firewall configurations can help protect a 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 must be evaluated case by case. MSM 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 network.

Specific links for access to an MSM system should not being sent by E-Mail. Hence, links into an MSM system contained in an email should not be opened. Suspicious emails should be reported to the IT administrator.

Frequently Asked Questions

What is MSM

The MSM is a monitoring system for high voltage switchgear.

What might an attacker use the vulnerability to do?

An attacker may use the vulnerability to trick a valid MSM user to download malicious software onto his computer or perform harmful command on MSM through its web server interface.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a forged link to the MSM web interface, of which the link directs to a malicious site. Prior knowledge on the MSM, the specific setup of the MSM in a substation and the contact of a target user are required. Furthermore, this exploitation can work for a user that already has an established session to the web interface.

Could the vulnerability be exploited remotely?

The vulnerabilities are not bound to a network stack. The vulnerability can be exploited from any terminal that has access to the MSM HTTP web interface.
When this security advisory was issued, had this vulnerability been publicly disclosed?

No, this vulnerability has not been publicly disclosed. Hitachi Energy received information about these vulnerabilities internally.

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

<table>
<thead>
<tr>
<th>Date of the Revision</th>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2022-07-12</td>
<td>A</td>
<td>Initial public release.</td>
</tr>
</tbody>
</table>