TLP:CLEAR
REVISION: 1
PUBLICATION DATE: 2023-04-25
DOC. IDENTIFIER: 8DBD000154
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Multiple Open-Source Software Related Vulnerabilities in Hitachi Energy's MSM Product

CVE-2021-43298
CVE-2020-15688
CVE-2019-16645
CVE-2019-12822
CVE-2018-15504
CVE-2018-15505
CVE-2021-41615
CVE-2023-23916

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of public reports of vulnerabilities related to open-source software components used in the MSM versions listed below. Please consult the Recommended Immediate Section for mitigation actions.

Vulnerabilities exist in the HTTP web user interface included in the product versions listed below.

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-2021-43298 Detail 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	The code that performs password matching when using 'Basic' HTTP authentication does not use a constant-time memcmp and has no rate-limiting. This means that an unauthenticated network attacker can brute-force the HTTP basic password, byte-by-byte, by recording the webserver's response time until the unauthorized (401) response.
CVE-2020-15688 Detail CVSS v3.1 Base Score: 8.8 High CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H Link to NVD: click here	The HTTP Digest Authentication in the GoAhead web server before 5.1.2 does not completely protect against replay attacks. This allows an unauthenticated remote attacker to bypass authentication via capture-replay if TLS is not used to protect the underlying communication channel.
CVE-2019-16645 Detail CVSS v3.1 Base Score: 8.6 High CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N Link to NVD: click here	An issue was discovered in Embedthis GoAhead 2.5.0. Certain pages (such as goform/login and config/log_off_page.htm) create links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker. This could potentially be used in a phishing attack.
CVE-2019-12822 Detail 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	In http.c in Embedthis GoAhead before 4.1.1 and 5.x before 5.0.1, a header parsing vulnerability causes a memory assertion, out-of-bounds memory reference, and potential DoS, as demonstrated by a colon on a line by itself.
CVE-2018-15504 Detail 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	An issue was discovered in Embedthis GoAhead before 4.0.1 and Appweb before 7.0.2. The server mishandles some HTTP request fields associated with time, which results in a NULL pointer dereference, as demonstrated by If-Modified-Since or If-Unmodified-Since with a month greater than 11.
CVE-2018-15505 Detail 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	An issue was discovered in Embedthis GoAhead before 4.0.1 and Appweb before 7.0.2. An HTTP POST request with a specially crafted "Host" header field may cause a NULL pointer dereference and thus cause a denial of service, as demonstrated by the lack of a trailing ']' character in an IPv6 address.

CVE-2021-41615 Detail 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	websda.c in GoAhead WebServer 2.1.8 has insufficient nonce entropy because the nonce calculation relies on the hardcoded onceuponatimeinparadise value, which does not follow the secret-data guideline for HTTP Digest Access Authentication in RFC 7616 section 3.3 (or RFC 2617 section 3.2.1). NOTE: 2.1.8 is a version from 2003; however, the affected websda.c code appears in multiple derivative works that may be used in 2021. Recent GoAhead software is unaffected.
CVE-2023-23916 Detail 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	An allocation of resources without limits or throttling vulnerability exists in curl <v7.88.0 based on the "chained" HTTP compression algorithms, meaning that a server response can be compressed multiple times and potentially with differentalgorithms. The number of acceptable "links" in this "decompression chain" wascapped, but the cap was implemented on a per-header basis allowing a maliciousserver to insert a virtually unlimited number of compression steps simply byusing many headers. The use of such a decompression chain could result in a "malloc bomb", making curl end up spending enormous amounts of allocated heap memory, or trying to and returning out of memory errors.

Affected Product Versions & Recommended Immediate Actions

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

Affected Version	Recommended Actions
MSM 2.2.5 and earlier	Apply general mitigation factors/workarounds.

Hitachi Energy recommends that customers apply the general mitigation measures as stated in this advisory.

General Mitigation Factors/Workarounds

MSM is not intrinsically designed and intended to be directly connected to the internet. Please disconnect the device from any internet facing network, if any installation has performed the same. Suggest adopting user access management and any state-of-the-art antivirus protection engines equipped with the latest signature rules on the computers that have installed and operating the MMS Client application. As an example, please use the Operating System (OS) inbuilt user access management functionality, if supported, to limit the probability of unauthorized access followed by rogue commands via MMS Client application.

Also, recommend following the hardening guidelines published by “The Center for Internet Security (CIS)” https://www.cisecurity.org/about-us/ to protect the host Operating System of computers that connects with MSM. This measure would then prevent the lateral movement of the attack vector into MSM via these connected devices. Some examples for Windows based computers are listed below.

1) CIS Microsoft Windows Desktop Benchmarks (cisecurity.org)
2) CIS Microsoft Windows Server Benchmarks (cisecurity.org)

Additional general mitigation factors are suggested below.

Recommended security practices and firewall configurations can help protect a network from attacks that originate from outside the network. Such practices include those 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. Monitoring 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.

Frequently Asked Questions

What is Modular Switchgear Monitoring (MSM)?

Condition monitoring for high-voltage switchgear. Modular Switchgear Monitoring (MSM) is used to supervise, manage and analyze performance of all types of high-voltage switchgear in new installations as well as a retrofit solution in existing high-voltage assets.

What is the scope of the vulnerability?

If an attacker is able to exploit these vulnerabilities as stated in this advisory, in the context of MSM, it can affect these below listed items.

1) Compromise the user access credentials of MSM HTTP web interface.
2) Make the MSM HTTP web interface unavailable, and thereby, causing a Denial-of-Service.

What might an attacker use the vulnerability to do?

An attacker successfully exploiting these vulnerabilities could perform these below listed operations.

1) Compromise the user access credentials and perform monitoring operations on MSM. Therefore, the monitored data from MSM could go into unsafe hands.
2) It can also try to upload a bogus firmware inside MSM but the probability that the rogue firmware would operate is significantly low because the firmware needs to be crated in accordance with the intrinsic embedded power system domain characteristics of MSM.

3) Can create Denial-of-Service on MSM HTTP web interface and make it unavailable.

How could an attacker exploit the vulnerability?

An attacker could exploit these vulnerabilities by either sending unsolicited emails containing specially crafted web links to the legitimate user or by getting access to the localized operational communication network of MSM. In the context of MSM, the vulnerability CVE-2021-43298 can only be exploited by an attacker by gaining access to the operational communication network of MSM i.e., the subnets where fleet of MSM are operating and by passively injecting a probe to monitor the response times to deduce the access credentials of legitimate users.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to MSM and or can deceive the legitimate users by making them click unsolicited emails pretending to contain legitimate information about MSM could remotely exploit these vulnerabilities as stated inside this advisory.

When this security advisory was issued, had these vulnerabilities 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 these vulnerabilities were being exploited?

No, Hitachi Energy had not received any information indicating that these vulnerabilities have 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
2023-04-25	1	Initial public release.

DocuSigned by: