Software Vulnerability Handling Policy
Table of contents

04  1. Introduction
   1.1. Purpose
   1.2. Scope

06  2. Product Security Incident Response Team

08  3. Vulnerability Disclosure Policy
   3.1. Reception
      3.1.1. Preferred Contact
      3.1.2. Content
      3.1.3. Secure Communication
      3.1.4. Acknowledgement of Reported Vulnerability
   3.2. Verification
   3.3. Remediation
   3.4. Cybersecurity Publication
      3.4.1. Publication Policy
      3.4.2. Types of Publication
      3.4.3. Publication Content
      3.4.4. Publication Timelines

15  4. Hitachi Energy is a CVE Numbering Authority

15  5. References
1. Introduction

Cybersecurity is a key priority for Hitachi Energy, and we are committed to providing secure products to our customers.

1.2. Scope of Vulnerability Handling

A vulnerability, according to ISO/IEC 29147 [1] is a behaviour or set of conditions present in a system, product, component, or service that violates an implicit or explicit security policy.

Such behavior or condition can be exploited and cause security issues. Any security issue may compromise the confidentiality, integrity, availability of the product or underlying system.

While Hitachi Energy assesses all reports of such occurrences, weaknesses in existing customer installations due to their individual designs, or compromised access credentials are not considered a Hitachi Energy vulnerability.

Furthermore, Hitachi Energy, at its sole discretion, will determine if end-of-life or unsupported products are covered by this policy.
2. Product Security Incident Response Team

The Hitachi Energy Product Security Incident Response Team (PSIRT) is a global team that receives, responds, and tracks any reported vulnerabilities, cybersecurity issues, and incidents related to our products.
3. Vulnerability Disclosure Policy

Hitachi Energy strives to follow Coordinated Vulnerability Disclosure (CVD) [2]. CVD is the process of gathering information from vulnerability finders, coordinating the sharing of that information between relevant stakeholders, and disclosing the existence of software vulnerabilities and their mitigations to various stakeholders, including the public.

CVD encourages the reporting of vulnerabilities without restrictions and provides the vendor the opportunity to investigate and remediate the vulnerability before the vulnerability is disclosed publicly. We believe that CVD helps our customers make more informed decisions about the actions that need to be taken by them to secure their systems from the reported vulnerabilities on our offerings. Importantly, we will continue to put the security interests of our customers at the center of any decisions we make.

Anyone discovering a software vulnerability affecting Hitachi Energy offerings is encouraged to contact Hitachi Energy directly. When the vulnerability is reported to us, it is important to also state whether the reporter is committed to coordinated disclosure.

The vulnerability disclosure and handling policy in our company is designed based on ISO/IEC 29147 [1] and ISO/IEC 30111 [3]. Hitachi Energy’s software vulnerability handling process has 4 stages: reception, verification, remediation, and publication.

If the reporting entity requests recognition, Hitachi Energy will acknowledge the reporting entity’s role, for instance, as part of official Hitachi Energy’s cybersecurity advisory.

At this time, Hitachi Energy does not have a bug bounty program, thus the acknowledgment of the reported vulnerability cannot be exchanged for monetary compensation.

Vulnerability report

1. RECEPTION
2. VERIFICATION
3. REMEDIATION
4. PUBLICATION
3.1. Reception

3.1.1. Preferred Contact
For any vulnerability discovered in Hitachi Energy products, the vulnerability reports can be submitted directly to Product Security Incident Response Team using the email address: cybersecurity@hitachienergy.com.

3.1.2. Content
To help in verifying the vulnerability, we expect the vulnerability report to include information that can help in reproducing the vulnerability internally. The information should have the following elements:

- Affected Hitachi Energy products
- Clear description of the vulnerability, including the necessary information required to identify the affected products
- Step-by-step instruction to reproduce the vulnerability
- Additional information, such as proof-of-concept scripts, screenshots, etc.
- Information on whether the vulnerability has been already published elsewhere

3.1.3. Secure Communication
Hitachi Energy recommends the use of PGP to securely transmit any sensitive data. The public PGP key for Hitachi Energy PSIRT can be found on the Cybersecurity web page at https://www.hitachienergy.com/cybersecurity under the section “Report an Incident or Vulnerability”.

In the event someone discovering a vulnerability relating to Hitachi Energy products does not wish to directly contact or interact with Hitachi Energy, we recommend contacting any CERT or other recognized coordinating organization.

3.1.4. Acknowledgement of Reported Vulnerability
When a vulnerability is reported to Hitachi Energy, we will formally acknowledge that the information is received. The vulnerability reporter will receive a written acknowledgment email including the name and contact information of the Hitachi Energy lead within seven calendar days. Additionally, the next possible correspondence timeline will be included in this first communication.

3.2. Verification

Any reported vulnerability in our offerings will be verified by the respective team and confirmed to the reporter.

During the verification stage, we will identify affected products and their support status, reproduce the vulnerability whenever possible and conduct a severity and impact assessment using the Common Vulnerability Scoring System (CVSS) v3.1 [4]. We will inform the reporter on the verification status and the next steps. The verification confirmation timeline will be created during the first email exchanges.

When we find a need for further coordination, for instance where a vulnerability involves/affected multiple parties, we will involve 3rd party coordination centers as necessary for further coordination.

1 PGP: Pretty Good Privacy
2 Computer Emergency Readiness Team, such as US-CERT CISA, or country specific CERT team.

cybersecurity@hitachienergy.com
www.hitachienergy.com/cybersecurity
3.3. Remediation

At this stage, the respective team will develop and validate software remediation and/or mitigations or workarounds. The type of remediation and the respective timeline will be defined according to several factors such as severity, affected products, current product lifecycle, etc. We will reassess the severity of the vulnerability (e.g., account for changes in publicly available information).

Our software remediation can be realized in one or more of the following types and the decision is based on different aforementioned factors, namely:

- A full patch or patch information
- A mitigation or workaround, which can include configuration changes (e.g., disabling of vulnerable service) or recommendations on deployment and configuration of security solutions (e.g., firewalls). It is Hitachi Energy’s goal to provide mitigations if possible, to offer customers alternatives to updating a running product immediately. Depending on the severity of the vulnerability and the time needed to develop a software remediation the alternative mitigations might be communicated before the final software remediation is available.

Hitachi Energy collaborates with reporting entities and government organizations to verify that remediations eliminate certain vulnerabilities and that the proposed mitigation alternatives effectively reduce risk.

3.4. Publication

3.4.1. Publication Policy

Hitachi Energy adheres to responsible disclosure principles that include the following:

- Cybersecurity advisories and notices that are made via publications. Vulnerability information is safeguarded until public release to protect the integrity of the product and prevent products from exploitation by malicious actors.
- Hitachi Energy extends the same responsible disclosure principles to its suppliers and vulnerability reporters.
- Hitachi Energy ranks the severity of vulnerabilities in accordance with Common Vulnerability Scoring System (CVSS).
- Hitachi Energy will publish vulnerability notification promptly. Priority will be afforded to the publication of vulnerabilities ranked high and critical in severity.
- Hitachi Energy follows responsible disclosure protocols in the publication of cybersecurity advisory and notifies all of its customers simultaneously by publishing the advisory in our Cybersecurity Alerts and Notifications page.

The followings are exceptions that justify an earlier publication of a cybersecurity advisory:

- There are indications that a vulnerability is being exploited or other malicious activity that would adversely affect customer cybersecurity.
- The existence of vulnerability is already generally known within the industry.

3.4.2. Types of Publication

Hitachi Energy may publish the following type of cybersecurity publication related to a vulnerability:

- Cybersecurity Advisory: a product specific publication related to one or multiple vulnerabilities to guide customers in mitigating risks of those vulnerabilities in our product(s) that are installed in their environment
- Cybersecurity Notification: a publication about one or multiple vulnerabilities that are released only on case-by-case basis prior to the completion of vulnerability verification activities on our offerings.

3.4.3. Publication Content

Cybersecurity advisories will provide summary documentation of vulnerabilities and material defects related to the procured product or services; the potential impact of such vulnerabilities and material defects, and the status of Hitachi Energy’s efforts to mitigate those publicly disclosed vulnerabilities and material defects, and our recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds. The published cybersecurity advisory may be accompanied with documentation from affected products that details more on the remediation information.

3.4.4. Publication Timelines

The cybersecurity advisory for the reported vulnerability will be published to the public after a mitigation strategy is defined. The cybersecurity advisory will be published on the Hitachi Energy – Cybersecurity – Alerts and Notification page. Subsequently, an email will be sent out to the users that subscribe to our Cybersecurity Alerts and Notification mailing list. To subscribe to our Cybersecurity Alerts and Notification, navigate to this link.
4. Hitachi Energy is a CVE Numbering Authority

As of June 2021, Hitachi Energy is authorized as a CNA (CVE Numbering Authority) [5] by the MITRE Corporation. With that said, Hitachi Energy has the authority to assign CVE-IDs to cybersecurity vulnerabilities found in its own offerings, regardless of whether it is internally or externally reported.

This move highlights our commitment to reporting and addressing any cybersecurity vulnerabilities in a timely manner and underscores our dedication to ensuring the integrity of power grids worldwide.

References


Hitachi Energy PSIRT
Email: cybersecurity@hitachienergy.com

©Hitachi Energy 2021. All rights reserved.
Specifications subject to change without notice.

Published in 2022.01.01

We reserve the right to make technical changes or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. Hitachi Energy Ltd. does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.

We reserve all rights in this document and in the subject matter and illustrations contained herein. Any reproduction, disclosure to third parties or utilization of its contents – in whole or in parts – is forbidden without prior written consent of Hitachi Energy Ltd.