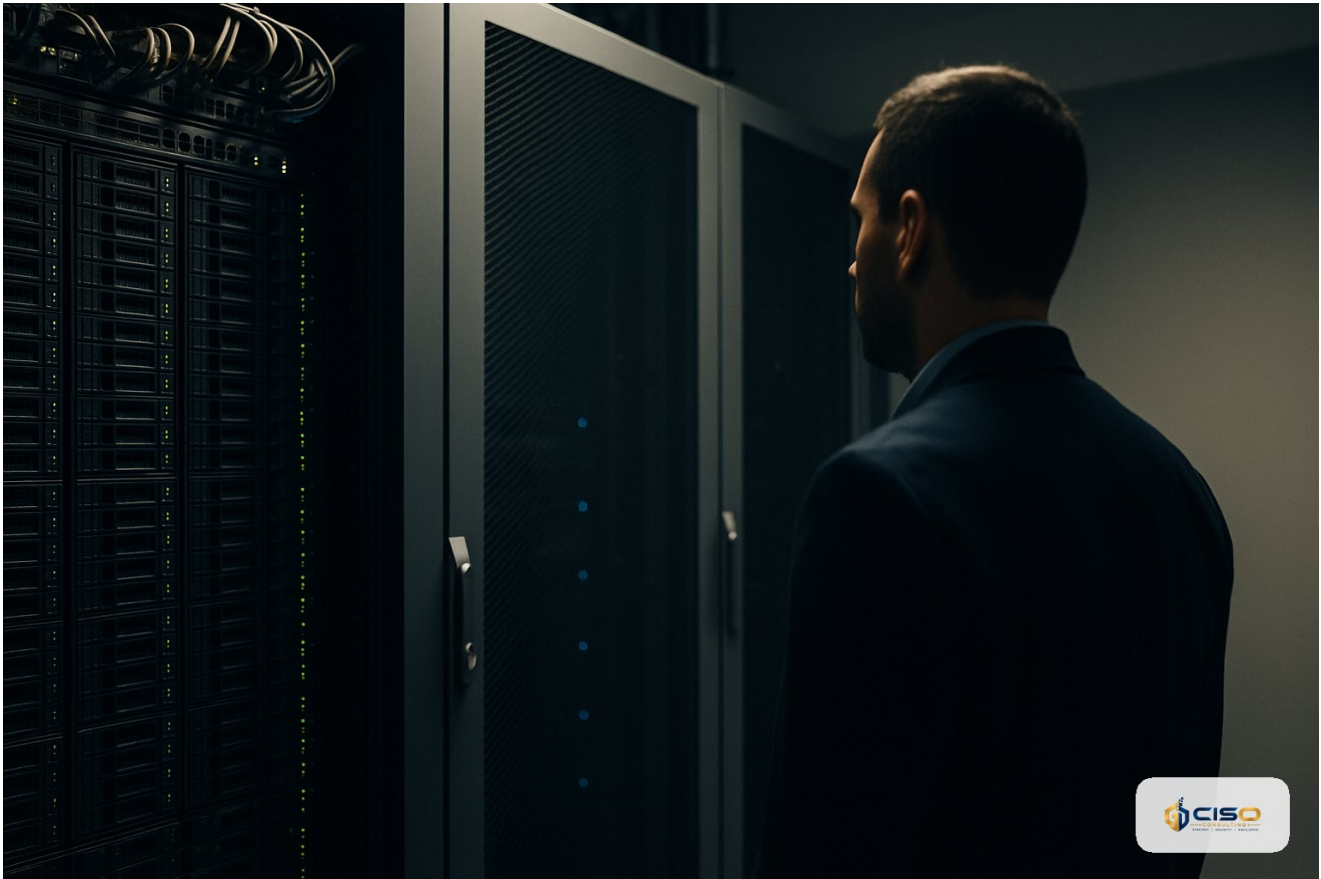


Advisory on Hitachi Energy SOI Vulnerability



Hitachi Energy has identified a ****Remote Code Execution**** vulnerability in the Apache ActiveMQ component of its SOI product. Institutions using affected versions should take immediate action to mitigate risks.

- The vulnerability affects SOI versions between 2.0.0 and 2.2.0.
- Exploitation may compromise the confidentiality, integrity, and availability of the product.
- Immediate action is recommended to mitigate potential risks.

Overview

Hitachi Energy has reported a **Remote Code Execution** vulnerability in the Apache ActiveMQ component of its SOI product. This issue affects specific versions of the SOI product, allowing potential attackers to exploit the vulnerability, which could lead to significant security risks.

Impact

The vulnerability can affect the **confidentiality**, **integrity**, and **availability** of the SOI product. Institutions utilizing the affected versions should be aware of the potential consequences and take necessary precautions to safeguard their systems.

Recommended Actions

To mitigate the risks associated with this vulnerability, organizations should take the following steps:

- Review the current version of the SOI product in use.
- Upgrade to a non-affected version of SOI as soon as possible.
- Implement security measures to restrict access to the Apache ActiveMQ component.
- Monitor systems for any unusual activity that may indicate exploitation attempts.
- Stay informed about updates and advisories from Hitachi Energy regarding this vulnerability.

What to do now

1. Review the current version of the SOI product in use.
2. Upgrade to a non-affected version of SOI as soon as possible.
3. Implement security measures to restrict access to the Apache ActiveMQ component.
4. Monitor systems for any unusual activity that may indicate exploitation attempts.
5. Stay informed about updates and advisories from Hitachi Energy regarding this vulnerability.