REVISION: C
PUBLICATION DATE: 2022-05-02
DOC. IDENTIFIER: 8DAA003540
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY NOTIFICATION

Spring4Shell and Spring Related Vulnerabilities

CVE-2022-22950
CVE-2022-22963
CVE-2022-22965

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of the Spring4Shell vulnerability (CVE-2022-22965 [1]) that was published on 2022-03-31. As published [2], under specific required conditions, exploitation of the vulnerabilities may lead to a remote-code execution. Additionally, we are also aware of two other vulnerabilities related to Spring Cloud and Spring Framework, namely CVE-2022-22963 [3] and CVE-2022-22950 [4] respectively.

Affected Products

We have completed the investigation of our products from our portfolio related to the afore-mentioned vulnerabilities. To date, the known affected product is listed below, and if the product is not listed, it is not vulnerable to the vulnerabilities.

– Lumada Asset Performance Management (affected only the Prognostic Model Executor Service)

General Mitigation Factors

Recommended security practices and firewall configurations can help protect a process control 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 have to be evaluated case by case. Process control 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 to a control system.

Support

For additional information and support please contact your product provider or Hitachi Energy's service organization. See https://www.hitachienergy.com/contact-us/ for Hitachi Energy contact-centers.

Publisher

Hitachi Energy PSIRT – cybersecurity@hitachienergy.com

References

1. https://tanzu.vmware.com/security/cve-2022-22965
2. https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement#am-i-impacted
3. https://tanzu.vmware.com/security/cve-2022-22963
4. https://tanzu.vmware.com/security/cve-2022-22950
5. https://www.cisa.gov/uscert/ncas/current-activity/2022/04/01/spring-releases-security-updates-addressing-spring4shell-and

Revision

Date of the Revision	Revision	Description
2022-04-01	A	Initial public release.
2022-04-04	B	Update references and summary.
2022-05-02	C	Concluded investigation and list an affected product.