April 5th, 2022
(Revision date: June 23rd, 2022)

To Our Valued Customers;

SAISON Information Systems Co., Ltd.
HULFT Technical Support Center

Regarding the Impact of the Spring Framework Vulnerability on Our Products

Thank you very much for using our technical support service.
We would like inform you of the impact of the Spring Framework vulnerability (CVE-2022-22965) disclosed on April 1, 2022, on HULFT and related products and our response policy.

For each product, we have listed the support of the latest version of the product.
This document will be updated and announced after the investigation is completed for products currently under investigation.

■HULFT/HULFT Manager

The module that causes this vulnerability is not in use and is therefore unaffected.

■HULFT Script

The module that causes this vulnerability is not in use and is therefore unaffected.

■HULFT-WebFileTransfer

The module that causes this vulnerability is not in use and is therefore unaffected.

■HDC-EDI Base/HDC-EDI Apex/HDC-EDI Manager

HDC-EDI Manager uses the Spring Framework. However, it is not affected by this vulnerability because it does not support JDK9 or higher environments.
This vulnerability does not affect other HDC products because the modules that cause this vulnerability are not used.

■iDIVO

The module that causes this vulnerability is not in use and is therefore unaffected.

■HULFT-WebConnect

Although it uses Spring Framework, it is not affected by this vulnerability because it is not used as a web application (packaged as a WAR file).

■HULFT IoT

Although it uses Spring Framework, it is not affected by this vulnerability because it is not used as a web application (packaged as a WAR file).

■DataMagic

The module that causes this vulnerability is not in use and is therefore unaffected.

■SIGNAlert

The module that causes this vulnerability is not in use and is therefore unaffected.

■HULFT-HUB

The module that causes this vulnerability is not in use and is therefore unaffected.

■DataSpider Servista、DataSpider Servista with Software Protection

Although Spring Framework is used, it is not affected by this vulnerability because it is embedded in JDK8.

■DataSpider Cloud

Although Spring Framework is used, it is not affected by this vulnerability because it is embedded in JDK8.
The service infrastructure part is not affected because the module that causes this vulnerability is not used.

■PIMSYNC

The module that causes this vulnerability is not in use and is therefore unaffected.

■DataSpider BPM

DataSpider BPM 2.6 is affected by this vulnerability because it uses the Spring Framework.
※Versions before 2.5 are not affected by this vulnerability because they are embedded in JDK8.

In response to this vulnerability, we are planning to release a patch to fix it.

・Scheduled release date: July 5th, 2022

■Thunderbus

The module that causes this vulnerability is not in use and is therefore unaffected.

■HULFT DataCatalog

Although it uses Spring Framework, it is not affected by this vulnerability because it is not used as a web application (packaged as a WAR file).

※Note

[Affected Vulnerability Information]

JPCERT/CC
Regarding Spring Framework Arbitrary Code Execution Vulnerability (CVE-2022-22965)
https://www.jpcert.or.jp/newsflash/2022040101.html

【Revision History】

April 5th, 2022	First edition created
April 13th, 2022	Reflected the investigation results of the HULFT DataCatalog.
May 6th, 2022	Reflected DataSpider BPM survey results
June 23rd, 2022	Listed the scheduled release date of the patch to fix DataSpider BPM

End