December 13, 2021
(Updated: December 15, 2021

Dear customers

Saison Information Systems Co., Ltd.
Customer service center
HULFT Technical Support Center

Regarding impact of Apache Log4j Vulnerability on HULFT Products

Dear Sir or Madam

Thank you very much for using our technical support service.
We would like to inform you of the impact of the Apache Log4j vulnerability (CVE-2021-44228) disclosed on December 10, 2021 on HULFT and related products and our response policy.

Yours sincerely

-Please note-

For each product, we will describe the correspondence of the latest version.
In addition, for products currently under investigation, we will update this document after the investigation is completed.

■HULFT

The module that causes this vulnerability is not used, so there is no impact.

■HULFT　Script

The module that causes this vulnerability is not used, so there is no impact.

■HULFT-WebFileTransfer

Currently under investigation.
The investigation is expected to be completed by December 17, 2021.

■HDC-EDI Base/HDC-EDI Manager

The module that causes this vulnerability is not used, so there is no impact.

■**iDIVO**

The module that causes this vulnerability is not used, so there is no impact.

■**HULFT-WebConnect**

The module that causes this vulnerability is not used, so there is no impact.

■**HULFT IoT**

The module that causes this vulnerability is not used, so there is no impact.

■**DataMagic**

The module that causes this vulnerability is not used, so there is no impact.

■**SIGNAlert**

The module that causes this vulnerability is not used, so there is no impact.

■**HULFT-HUB**

The module that causes this vulnerability is not used, so there is no impact.

■**DataSpider Servista with Software Protection**

The module that causes this vulnerability is not used, so there is no impact.

※remarks

[Vulnerability information]

US-CERT - CISA

Apache Log4j allows insecure JNDI lookups

https://kb.cert.org/vuls/id/930724

END