May 19th, 2023

To Our Valued Customers;

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

Regarding the vulnerability in ScriptRunner and ScriptRunner for Amazon SQS in DataSpider Servista

Thank you very much for using our technical support service.
It has been discovered that there is a private key hard-coded issue (CWE-321) for ScriptRunner and ScriptRunner for Amazon SQS in DataSpider Servista.
This vulnerability has been fixed in the latest release of DataSpider Servista (service pack・patch module.) Please check the following information if you are using ScriptRunner or ScriptRunner for Amazon SQS.

1. Applicable Products and Versions

- DataSpider Servista Advanced Server Package
- DataSpider Servista Basic Server Package
- DataSpider Servista Select

All versions are eligible.

2. Range of Impact

- ScriptRunner
- ScriptRunner for Amazon SQS

You are not affected if you are not using ScriptRunner or ScriptRunner for Amazon SQS (have not created a startup configuration file).

3. Impact of Vulnerability

An attacker with access to the product in question could decrypt encrypted credentials using a hard-coded encryption key if they obtain the ScriptRunner or ScriptRunner for Amazon SQS startup configuration file.

4. Requests to Customers

Please apply the corresponding patch module and perform the necessary procedures for the startup configuration file. Please refer to the README included with the patch module for details on the procedure.

Patch modules can be downloaded from myHULFT.

The corresponding patch modules for each version you are using are as follows:

DataSpider Servista Version	Supported Service Packs and Patch Modules	Note
4.4	4.4SP1	4.4SP1 is a service pack that has completed support for this issue.
4.3	Patch for 4.3SP2 「DSS43SP2_221005_05」	If 4.3SP2 has not been applied, please apply this patch after using SP2.
4.2	Patch for 4.2SP9 「DSS42SP9_221005_05」	If 4.2SP9 has not been applied, please apply this patch after using SP9.

If you are using DataSpider Servista 4.1 or lower, please apply the above patch module after upgrading to 4.2 or higher.

5. Contact for Inquiries Regarding this Information

Please contact your technical support service contractor.

End

【Revision History】

May 19th, 2023	First edition created

Appendix: FAQs and Answers

Q1	How do I check if ScriptRunner is used?

A：

ScriptRunner executes a script by running ScriptRunner.exe with a startup configuration file as a command line argument. For details, please refer to the help page at the URL below.

[ScriptRunner]

URL：https://www.hulft.com/help/ja-jp/DataSpider/dss44sp1/help/ja/tools/scriptrunner.html

For this reason, please check below if ScriptRunner is used or not.

- Whether you have the ScriptRunner.exe installed in your environment or not.
- Whether you are operating in the above environment to execute a script with ScriptRunner.exe by specifying a startup configuration file created by the customer or not.

Q2	I do not use ScriptRunner, but ScriptRunner.exe and ScriptRunnerSQS.exe exist in the DataSpiderServer operating environment. Does this vulnerability issue occur if these two files exist in the DataSpiderServer operating environment?

A：

This vulnerability is related to the encryption of the startup configuration file used to execute scripts in ScriptRunner and ScriptRunner for Amazon SQS.

Therefore, even if the ScriptRunner.exe and ScriptRunnerSQS.exe files exist, they will not be affected if the startup configuration file is not created.

Q3	Since the patch will be released for DataSpider Servista 4.4, 4.3, and 4.2, is it necessary to upgrade if I use 4.1 or lower?

A：

We apologize for the inconvenience, but please upgrade to DataSpider Servista 4.2 or later.

DataSpider Servista 4.1 has been supported by Assistance Support since July 5th, 2022, and no patches will be provided.

Q4	Have there been any actual cases of this vulnerability causing damage?

A：
We have not received any reports of damage caused by this vulnerability at this time.

Q5	Is there any way to confirm that the behavior has improved as expected after applying the patch?

A：
Execute ScriptRunner.exe using a startup configuration file that has not been changed since before the patch was applied. If an error occurs, the patch has been applied.

In response to this vulnerability, we have made changes to store the encryption key for decrypting the authentication information in the execution environment. As a result, the authentication information in the startup configuration file before the patch is applied cannot be decrypted after the patch is applied, resulting in an error.

Q6	Is it correct to understand that if a machine with the DataSpider Servista installed is not communicating using ScriptRunner, it is not affected by the vulnerability?

A：
This vulnerability allows an attacker with access to the DataSpiders deployment environment to verify credentials if they obtain the ScriptRunner startup configuration file.
Even if there is no communication between ScriptRunner and DataSpiderServer, if a pre-created startup configuration file exists, it will be affected when the file is obtained.

Q7	How do I apply the service pack?

A：
The service packs are located in the directory "ServicePack" on the same level as the installer package downloaded from myHULFT.

The service pack is provided in a compressed ZIP format "DSSxx_SPx.zip".
Please refer to "DSSxx_SPx_README_en.txt" in the decompressed folder and apply the service pack. Also, please refer to the documentation in the decompressed folder for details about additional feature patches and service packs.

Q8	When applying the latest Service Pack (SP), will the contents of the previous SP also be applied if I apply the latest SP without applying the previous SP?

A：

Even if the latest SP is applied without the past SPs, all SP contents, including the past SPs, will be applied. (If the latest SP is SP9, and SP9 is applied without SP1-8, all SP contents from SP1 to SP9 will be applied.)

Therefore, applying SP1, SP2, … SP9 in that order is unnecessary.

End