May 19th, 2023

To Our Valued Customers;

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

Regarding the HULFT8 Script Options ScriptRunner containing a vulnerability

Thank you very much for using our technical support service.
It has been discovered that there is an issue (CWE-321) with the ScriptRunner in HULFT8 Script Option where the private key is hard coded.
This vulnerability has been addressed in a modified patch for HULFT8 Script Option; if you are using ScriptRunner, please check the following information and consider addressing this issue.

1. **Applicable Products and Versions**
   - HULFT8 Script Option for Windows/UNIX/Linux

   All versions are eligible.

2. **Range of Impact**
   - ScriptRunner

   If ScriptRunner is not used (no startup configuration file is created), there is no impact.

3. **Impact of Vulnerability**
   An attacker with access to the product in question could use a hard-coded encryption key to decrypt encrypted credentials if they obtain the ScriptRunner startup configuration file.

4. Requests to Customers

The modified patch to correct this vulnerability can be applied to HULFT8 Script Option Ver. 8.5.3. Therefore, if you are using Ver. 8.5.2 or lower, please update to Ver. 8.5.3. After that, please apply the following modified patch.

HULFT8 Script Option Version	Corresponding modified patch module	Note
8.5.3	HS85_230508_02	

The modified patch above is available on myHULFT.

You can download it by selecting the product from the "Product Download/Issue Key" menu.

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

【Notes】

The HULFT main unit and HULFT8 Script Option must be used at the same level※.

Therefore, when upgrading HULFT8 Script Option to Ver. 8.5.3, HULFT itself must also be upgraded to Ver. 8.5.X.

※In the case of Ver. X.Y.Z, the "Y" part is level.

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 being used?

A：

ScriptRunner executes a script by running ScriptRunner.exe with a startup configuration file as a command line argument. Please refer to the following in the HULFT8 Script Option online help for details.

<Online Help>
  [Operation Tool]-[ScriptRunner]

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 is in the HULFT8 Script Option operating environment. Does this vulnerability issue occur when this file is in the HULFT8 Script Option operating environment?

A：

This vulnerability is related to password encryption of the startup configuration file used to execute scripts in ScriptRunner.

Therefore, even if the ScriptRunner.exe file exists, it will not be affected if the startup configuration file is not created.

Q3	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.

Q4	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 changed to store the encryption key for decrypting authentication information in the execution environment. As a result, passwords in the startup configuration file before the patch was applied cannot be decrypted after the patch was applied, resulting in an error.

Q5	Is it correct to understand that if a machine with the HULFT8 Script Option installed is not communicating using ScriptRunner, it is not affected by the vulnerability?

A：

This vulnerability allows an attacker with access to the HULFT8 Script Options deployment environment to verify credentials if they obtain the ScriptRunner startup configuration file.
Even if there is no communication between ScriptRunner and HULFT8 Script Option, if a pre-created startup configuration file exists, it will be affected when the file is obtained.

End