Phụ lục

THÔNG TIN LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số /CATTT-NCSC ngày / /2022 của Cục An toàn thông tin)

1. Thông tin lỗ hổng bảo mật

- Mô tả: Lỗ hổng ảnh hưởng đến sản phẩm WSO2 cho phép đối tượng tấn công thực thi mã từ xa trên máy chủ.

- CVSS: 9.8 (Nghiêm trọng)

- Ảnh hưởng:

- ✓ WSO2 API Manager phiên bản 2.2.0 trở lên;
- ✓ WSO2 Identity Server phiên bản 5.2.0 trở lên;
- ✓ WSO2 Identity Server Analytics phiên bản 5.4.0, 5.4.1, 5.5.0, 5.6.0;
- ✓ WSO2 Identity Server as Key Manager phiên bản 5.3.0 trở lên;
- ✓ WSO2 Enterprise Integrator phiên bản 6.2.0 trở lên.

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục lỗ hổng này là nâng cấp lên phiên bản mới nhất. Trong trường hợp không thể nâng cấp do chưa có phát hành phiên bản mới tương ứng với phiên bản đang sử dụng, Quý đơn vị có thể áp dụng các bản sửa lỗi liên quan dựa trên các bản sửa lỗi đã công khai được cung cấp dưới đây:

https://github.com/wso2/carbon-kernel/pull/3152

https://github.com/wso2/carbon-identity-framework/pull/3864

https://github.com/wso2-extensions/identity-carbon-auth-rest/pull/167

Ngoài ra để giảm thiểu nguy cơ tấn công, Quý đơn vị có thể thực hiện các bước khắc phục thay thế tạm thời như sau:

Phiên bản bị ảnh hưởng	**Các bước khắc phục thay thế**
WSO2 API Manager 2.6.0, 2.5.0, 2.2.0 WSO2 Identity Server 5.8.0, 5.7.0, 5.6.0, 5.5.0, 5.4.1, 5.4.0, 5.3.0, 5.2.0 WSO2 Identity Server as Key Manager 5.7.0, 5.6.0, 5.5.0, 5.3.0	Xóa tất cả mapping defined bên trong FileUploadConfig tag tại: <product_home>/repository/conf/carbon.xml

<table>
<tr><td>WSO2 IS Analytics 5.6.0, 5.5.0, 5.4.1, 5.4.0</td><td></td></tr>
<tr><td>WSO2 API Manager 4.0.0, 3.2.0, 3.1.0, 3.0.0</td><td>Thêm cấu hình dưới đây vào <product_home>/repository/conf/deployment.toml

deployment.toml

[[resource.access_control]]
context="(.*)/fileupload/resource(.*)"
secure=false
http_method = "all"

[[resource.access_control]]
context="(.*)/fileupload/(.*)"
secure=true
http_method = "all"
permissions = ["/permission/protected/"]</td></tr>
<tr><td>WSO2 Identity Server 5.11.0, 5.10.0, 5.9.0
WSO2 Identity Server as Key Manager 5.10.0, 5.9.0</td><td>Thêm cấu hình dưới đây vào <product_home>/repository/conf/deployment.toml

deployment.toml

[[resource.access_control]]
context="(.*)/fileupload/service(.*)"
secure=false
http_method = "all"

[[resource.access_control]]
context="(.*)/fileupload/entitlement-policy(.*)"
secure=false
http_method = "all"

[[resource.access_control]]
context="(.*)/fileupload/resource(.*)"
secure=false
http_method = "all"

[[resource.access_control]]
context="(.*)/fileupload/(.*)"
secure=true
http_method = "all"</td></tr>
</table>

	permissions = ["/permission/protected/"]
WSO2 Enterprise Integrator 6.6.0, 6.5.0, 6.4.0, 6.3.0, 6.2.0	Đối với EI profile, xóa mappings trong tệp <product_home>/conf/carbon.xml ra khỏi <FileUploadConfig> Đối với Business process / Broker và Analytics profiles, thay đổi lại tệp carbon.xml cho các vị trí tương ứng sau: <product_home>/wso2/broker/conf/carbon.xml <product_home>/wso2/business-process/conf/carbon.xml <product_home>/wso2/analytics/conf/carbon.xml **deployment.toml** <Mapping> <Actions> <Action>keystore</Action> <Action>certificate</Action> <Action>*</Action> </Actions> <Class>org.wso2.carbon.ui.transports.fileupload.AnyFileUploadExecutor</Class> </Mapping> <Mapping> <Actions> <Action>jarZip</Action> </Actions> <Class>org.wso2.carbon.ui.transports.fileupload.JarZipUploadExecutor</Class> </Mapping> <Mapping> <Actions> <Action>tools</Action> </Actions> <Class>org.wso2.carbon.ui.transports.fileupload.ToolsFileUploadExecutor</Class> </Mapping> <Mapping>

	<Actions> <Action>toolsAny</Action> </Actions> <Class>org.wso2.carbon.ui.transports.fileupload.ToolsAnyFileUploadExecutor</Class> </Mapping>

3. Nguồn tham khảo

https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2021-1738