UBND TỈNH HÀ NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 427 /STTTT-BCVTCNTT

V/v nguy cơ tấn công vào hệ thống thông tin của các cơ quan, tổ chức thông qua lỗ hổng bảo mật CVE-2022-29464

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nam, ngày 20 tháng 4 năm 2022

Kính gửi:

- Văn phòng Tỉnh ủy Hà Nam;
- Các sở, ban, ngành, cơ quan, đoàn thể của tỉnh;
- UBND các huyện, thị xã, thành phố.

Căn cứ Công văn số 548/CATTT-NCSC ngày 19/4/2022 của Cục An toàn thông tin, Bộ Thông tin và Truyền thông về việc nguy cơ tấn công vào hệ thống thông tin của các cơ quan, tổ chức thông qua lỗ hổng bảo mật CVE-2022-29464;

Nhằm tăng cường công tác bảo đảm an toàn, an ninh thông tin, đặc biệt là bảo vệ các hệ thống thông tin của các cơ quan, đơn vị trên địa bàn tỉnh để góp phần bảo đảm bảo an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị:

- Kiểm tra, rà soát và xác minh hệ thống thông tin có sử dụng sản phẩm WSO2. Trong trường hợp bị ảnh hưởng, cần thực hiện nâng cấp lên phiên bản mới nhất hoặc thực hiện các biện pháp khắc phục thay thế nhằm giảm thiểu nguy cơ bị tấn công *(Chi tiết tại phụ lục kèm theo)*.

- Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

Đầu mối liên hệ, hỗ trợ:

- Sở Thông tin và Truyền thông (Trung tâm Công nghệ thông tin và Truyền thông - Bộ phận thường trực Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh Hà Nam). Điện thoại: **0226.3846333**. Email: **ttcntt@hanam.gov.vn**

- Trung tâm Giám sát an toàn thông tin mạng quốc gia (NCSC), Cục An toàn thông tin. Điện thoại di động: **0243.2091616**. Email: **ais@mic.gov.vn**./.

Nơi nhận:
- Như trên;
- Lưu VT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XHCN VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH HÀ NAM

Nguyễn Đức Cường

Phụ lục

THÔNG TIN VỀ LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số /STTTT-BCVTCNTT ngày / /2022 của Sở Thông tin và Truyền thông Hà Nam)

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 kiểm tra và khắc phục lỗ hổng

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, các cơ quan, 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, các cơ quan, 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 WSO2 IS Analytics 5.6.0, 5.5.0, 5.4.1, 5.4.0	Xóa tất cả mapping defined bên trong FileUploadConfig tag tại: <product_home>/repository/conf/carbon.xml

<table>
<tr><th>Phiên bản bị ảnh hưởng</th><th>Các bước khắc phục thay thế</th></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"
permissions = ["/permission/protected/"]</td></tr>
</table>

<table>
<tr><th>Phiên bản bị ảnh hưởng</th><th>Các bước khắc phục thay thế</th></tr>
<tr><td>WSO2 Enterprise Integrator 6.6.0, 6.5.0, 6.4.0, 6.3.0, 6.2.0</td><td>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></td></tr>
</table>

Phiên bản bị ảnh hưởng	Các bước khắc phục thay thế
	</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