UBND TỈNH QUẢNG NGÃI
SỞ GIÁO DỤC VÀ ĐÀO TẠO

Số: 467 /TB-SGDĐT

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

Quảng Ngãi, ngày 22 tháng 4 năm 2022

THÔNG BÁO
Nguy cơ tấn công vào hệ thống thông tin của cơ sở giáo dục thông qua lỗ hổng bảo mật CVE-2022-29464

Theo đề nghị của Sở Thông tin và Truyền thông tại Công văn số 498/STTTT-BCVT&CNTT ngày 21/4/2022 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;

Sở Giáo dục và Đào tạo thông báo đến các đơn vị, cơ sở giáo dục nắm tình hình, triển khai thông tin đến các cán bộ, giáo viên thực hiện các biện pháp để hạn chế các rủi ro về nguy cơ mất an toàn thông tin. *(Kèm theo Công văn số 498/STTTT-BCVT&CNTT ngày 21/4/2022 của Sở Thông tin và Truyền thông)*

Yêu cầu lãnh đạo các đơn vị quan tâm chỉ đạo thực hiện./.

***Nơi nhận*:**
- Đơn vị trực thuộc Sở GDĐT;
- Phòng GDĐT huyện, thị xã, thành phố;
- Trung tâm GDNN-GDTX huyện, thị xã;
- Lãnh đạo Sở GDĐT;
- Các phòng thuộc Sở GDĐT;
- Lưu: VT, VP, ndh.

TL. GIÁM ĐỐC
KT. CHÁNH VĂN PHÒNG
PHÓ CHÁNH VĂN PHÒNG

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH QUẢNG NGÃI

Nguyễn Đức Huân

UBND TỈNH QUẢNG NGÃI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số:498 /STTTT-BCVT&CNTT

Quảng Ngãi, ngày 21tháng 4 năm 2022

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

Kính gửi:
- Văn phòng: Tỉnh ủy, Đoàn ĐBQH&HĐND, UBND tỉnh;
- Các sở, ban, ngành; Hội, đoàn thể tỉnh;
- UBND các huyện, thị xã, thành phố;
- Báo Quảng Ngãi, Đài Phát thanh và Truyền hình tỉnh.

Theo cảnh báo của Cục An toàn thông tin tại Công văn số 548/CATTT-NCSC ngày 19/4/2022 nguy cơ tấn công vào hệ thống thông tin của các cơ quan, tổ chức thông qua lỗ hổng bảo mật CVE-2022-29464; Sở Thông tin và Truyền thông đề nghị lãnh đạo các cơ quan, đơn vị, địa phương chỉ đạo thực hiện một số biện pháp sau để hạn chế các rủi ro về nguy cơ mất an toàn thông tin:

1. Kiểm tra, rà soát và xác minh hệ thống thông tin của cơ quan, đơn vị có sử dụng sản phẩm WSO2. Trong trường hợp bị ảnh hưởng, các đơn vị cần nâng cấp lên phiên bản mới nhất hoặc thực hiện các biện pháp khắc phục thay thế nhằm giảm thiểu nguy cơ tấn công.

(Tham khảo hướng dẫn tại Phụ lục đính kèm Công văn này).

2. 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.

3. Khi phát hiện các hệ thống có biểu hiện bị khai thác, tấn công mạng, triển khai ngay các biện pháp xử lý ngăn chặn tấn công trên hệ thống và thông báo về Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi để có các biện pháp hỗ trợ, xử lý kịp thời.

Đề nghị lãnh đạo các cơ quan, đơn vị, địa phương quan tâm chỉ đạo thực hiện./.

***Nơi nhận*:**
- Như trên;
- Phòng VH&TT các huyện, thị xã, thành phố;
- Thành viên Đội ứng cứu sự cố ATTT mạng tỉnh;
- Sở TT&TT: Lãnh đạo Sở, các phòng chuyên môn, TT CN-TT&TT;
- Lưu: VT, BCVT&CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH QUẢNG NGÃI

Đỗ Quang Nghĩa

PHỤ LỤC
Thông tin lỗ hổng bảo mật

(Kèm theo Công văn số /STTTT-BCVT&CNTT ngày /4/2022 của Sở Thông tin và Truyền thông)

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 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, 5.9.0WSO2 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>
<tr><td>WSO2 Enterprise Integrator 6.6.0,</td><td>Đối với EI profile, xóa mappings trong tệp <product_home>/conf/carbon.xml ra khỏi</td></tr>
</table>

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

Phiên bản bị ảnh hưởng	Các bước khắc phục thay thế
	ToolsAnyFileUploadExecutor</Class> </Mapping>

3. Nguồn tham khảo

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