UBND TỈNH ĐỒNG NAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 1134 /STTTT-CNTTVT

Đồng Nai, ngày 17 tháng 5 năm 2022

V/v 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

Kính gửi:
- Các cơ quan đảng, nhà nước trên địa bàn tỉnh;
- Các tổ chức chính trị - xã hội thuộc địa bàn tỉnh;
- Viettel Đồng Nai, VNPT Đồng Nai, Mobifone Đồng Nai;
- Trung tâm Công nghệ thông tin tỉnh Đồng Nai.

Sở Thông tin và Truyền thông nhận văn bản 548/CATTT-NCSC ngày 19/4/2022 của Cục An toàn thông tin 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;

Theo văn bản trên, ngày 01/4/2022, WSO2 đã công bố lỗ hổng bảo mật CVE-2022-29464 (WSO2-2021-1738) ảnh hưởng đến các sản phẩm của WSO2 bao gồm WSO2 API Manager, WSO2 Identity Server, WSO2 Enterprise Integrator. Lỗ hổng này có điểm CVSS: 9.8 (Nghiêm trọng) cho phép đối tượng tấn công tải tệp tùy ý lên máy chủ từ đó thực thi mã từ xa.

WSO2 cung cấp các sản phẩm phần mềm mã nguồn mở thường được sử dụng nhiều trong các cơ quan tổ chức có hệ thống thông tin với quy mô lớn như một giải pháp chia sẻ dữ liệu tập trung. Vì vậy theo đánh giá sơ bộ của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin mức độ ảnh hưởng của lỗ hổng này rất lớn.

Để tăng cường đảm bảo an toàn thông tin mạng trên địa bàn tỉnh, góp phần bảo đảm bảo an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông đề nghị Quý đơn vị chủ động thực hiện các biện pháp sau:

1. Kiểm tra, rà soát và xác minh hệ thống thông tin có sử dụng sản phẩm WSO2. Trong trường hợp bị ảnh hưởng, Quý 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 có tại phụ lục kèm theo).

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. Trong trường hợp cần hỗ trợ, Quý đơn vị liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại: 02432091616, thư điện tử: ncsc@ais.gov.vn hoặc Sở Thông tin và

Truyền thông, điện thoại 0251.3810.269, thư điện tử: attt@dongnai.gov.vn./.

Trân trọng./.

Nơi nhận:
- Như trên;
- UBND tỉnh (b/c);
- Giám đốc và Phó Giám đốc Sở;
- Lưu: VT, CNTTVT, Thịnh.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH ĐỒNG NAI

Võ Hoàng Khai

Phụ lục

THÔNG TIN LỖ HỔNG BẢO MẬT

(Kèm theo văn bản số 1134/STTTT-CNTTVT ngày 17 /5/2022 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	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"
permissions = ["/permission/protected/"]</td></tr>
</table>

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