BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Số: 130 /TTCNTT-KTHT
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 Nội, ngày 27 tháng 04 năm 2022

Kính gửi: Các đơn vị trực thuộc Bộ

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 Cục An toàn thông tin – Bộ Thông tin và Truyền thông mức độ ảnh hưởng của lỗ hổng này rất lớn.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, Trung tâm Công nghệ thông tin khuyến nghị Quý đơn vị thực hiện:

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.

Trong trường hợp cần thiết, Quý đơn vị liên hệ đầu mối hỗ trợ của Trung tâm Công nghệ thông tin: Phòng Kỹ thuật hạ tầng, điện thoại 024.39439060, thư điện tử: phongktht@most.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Bùi Thế Duy (để b/c);
- Cổng thông tin điện tử Bộ KH&CN;
- Lưu: VT, KTHT.

GIÁM ĐỐC

TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Hà Quốc Trung

PHỤ LỤC
THÔNG TIN LỖ HỔNG BẢO MẬT
(Kèm theo Công văn số 130/TTCNTT-KTHT ngày 27 /04 /2022 của Trung tâm Công nghệ 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

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN

(Kèm theo Công văn số 130 /TTCNTT-KTHT ngày 27 /04 /2022 của Trung tâm Công nghệ thông tin)

TT	Tên đơn vị
1.	Thanh tra Bộ
2.	Cục Công tác phía Nam
3.	Cục Ứng dụng và phát triển công nghệ
4.	Cục Năng lượng nguyên tử
5.	Cục Thông tin Khoa học và Công nghệ Quốc gia
6.	Cục Phát triển thị trường và doanh nghiệp khoa học và công nghệ
7.	Cục An toàn bức xạ và hạt nhân
8.	Cục Sở hữu trí tuệ
9.	Tổng Cục tiêu chuẩn đo lường chất lượng
10.	Ban quản lý khu công nghệ cao Hoà Lạc
11.	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo
12.	Viện Khoa học và công nghệ Việt Nam - Hàn Quốc (VKIST)
13.	Viện Nghiên cứu sáng chế và Khai thác công nghệ
14.	Viện Năng lượng nguyên tử Việt Nam
15.	Viện Ứng dụng công nghệ
16.	Viện Đánh giá khoa học và Định giá công nghệ
17.	Viện Khoa học sở hữu trí tuệ
18.	Viện Nghiên cứu và Phát triển Vùng
19.	Văn phòng các Chương trình trọng điểm cấp nhà nước
20.	Văn phòng Công nhận chất lượng
21.	Văn phòng Đăng ký hoạt động khoa học và công nghệ
22.	Văn phòng các Chương trình khoa học và công nghệ quốc gia
23.	Báo Khoa học và Phát triển
24.	Tạp chí Khoa học và Công nghệ Việt Nam
25.	Nhà xuất bản Khoa học và Kỹ thuật
26.	Quỹ Phát triển khoa học và công nghệ quốc gia
27.	Quỹ Đổi mới công nghệ quốc gia
28.	Trung tâm Nghiên cứu và Phát triển truyền thông khoa học và công nghệ
29.	Trung tâm Nghiên cứu và Phát triển hội nhập khoa học và công nghệ quốc tế