UBND TỈNH LAI CHÂU
**SỞ THÔNG TIN VÀ TRUYỀN THÔNG**

Số595 /STTTT-BCVTCNTT
V/v cảnh báo 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**

*Lai Châu, ngày 21 tháng 4 năm 2022*

Kính gửi:
- Các Sở, ban, ngành, đoàn thể tỉnh;
- UBND các huyện, thành phố;
- Ngân hàng nhà nước chi nhánh tỉnh Lai Châu;
- Kho bạc nhà nước;
- Các doanh nghiệp viễn thông, CNTT.

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.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý cơ quan, góp phần bảo đảm an toàn cho không gian mạng, Sở Thông tin và Truyền thông đề nghị quý cơ quan 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.

3. Nếu phát hiện vấn đề nghiêm trọng về lỗ hổng trên, báo cáo về Sở

Thông tin và Truyền thông để có biện pháp khắc phục, xử lý kịp thời theo số điện thoại: 02133798798 hoặc 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.

Trân trọng./.

***Nơi nhận:***
- Như trên;
- Lưu: VT, BCVTCNTT.

**GIÁM ĐỐC**

Ký bởi: Sở Thông tin và Truyền thông
Thời gian ký: 21/04/2022 16:16:37

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH LAI CHÂU

**Nguyễn Minh Hiệu**

**PHỤ LỤC**

**Thông tin về các lỗ hổng bảo mật ảnh hưởng đến sản phẩm WSO2**

*(Kèm theo công văn số /STTTT-BCVTCNTT ngày tháng năm 2022)*

**1. Thông tin các lỗ hổng bảo mật**

**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<br>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<br>WSO2 Identity Server as Key Manager 5.7.0, 5.6.0, 5.5.0, 5.3.0<br>WSO2 IS Analytics 5.6.0, | Xóa tất cả mapping defined bên trong FileUploadConfig tag tại:<br>**<product_home>/repository/conf/carbon.xml** |

<table>
<tr><td>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<br><br>deployment.toml<br><br>[[resource.access_control]]<br>context="(.*)/fileupload/resource(.*)"<br>secure=false<br>http_method = "all"<br><br>[[resource.access_control]]<br>context="(.*)/fileupload/(.*)"<br>secure=true<br>http_method = "all"<br>permissions = ["/permission/protected/"]</td></tr>
<tr><td>WSO2 Identity Server 5.11.0, 5.10.0, 5.9.0<br>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<br><br>deployment.toml<br><br>[[resource.access_control]]<br>context="(.*)/fileupload/service(.*)"<br>secure=false<br>http_method = "all"<br><br>[[resource.access_control]]<br>context="(.*)/fileupload/entitlement-policy(.*)"<br>secure=false<br>http_method = "all"<br><br>[[resource.access_control]]<br>context="(.*)/fileupload/resource(.*)"<br>secure=false<br>http_method = "all"<br><br>[[resource.access_control]]<br>context="(.*)/fileupload/(.*)"<br>secure=true<br>http_method = "all"<br>permissions = ["/permission/protected/"]</td></tr>
</table>

<table>
<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><br>Đối với Business process / Broker và Analytics profiles, thay đổi lại tệp carbon.xml cho các vị trí tương ứng sau:<br><product_home>/wso2/broker/conf/carbon.xml<br><product_home>/wso2/business-process/conf/carbon.xml<br><product_home>/wso2/analytics/conf/carbon.xml<br><br>deployment.toml<br><br><Mapping><br><Actions><br><Action>keystore</Action><br><Action>certificate</Action><br><Action>*</Action><br></Actions><br><Class>org.wso2.carbon.ui.transports.fileupload.AnyFileUploadExecutor</Class><br></Mapping><br><br><Mapping><br><Actions><br><Action>jarZip</Action><br></Actions><br><Class>org.wso2.carbon.ui.transports.fileupload.JarZipUploadExecutor</Class><br></Mapping><br><br><Mapping><br><Actions><br><Action>tools</Action><br></Actions><br><Class>org.wso2.carbon.ui.transports.fileupload.ToolsFileUploadExecutor</Class><br></Mapping><br><br><Mapping><br><Actions><br><Action>toolsAny</Action><br></Actions><br><Class>org.wso2.carbon.ui.transports.fileupload.ToolsAnyFileUploadExecutor</Class><br></Mapping></td>
</tr>
</table>

### 3. Nguồn tham khảo

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