

SỞ THÔNG TIN VÀ TRUYỀN  
THÔNG THANH HÓA  
**TRUNG TÂM CNTT&TT**

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

Số: /TTCNTT&TT-QTHT

Thanh Hoá, ngày tháng 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;
- Văn Phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn Phòng UBND tỉnh;
- Các sở, ban, ngành cấp tỉnh;
- UBND các huyện, thị xã, thành phố;
- Các tổ chức đoàn thể chính trị cấp tỉnh;
- Các doanh nghiệp viễn thông, CNTT trên địa bàn tỉnh.

Căn cứ Công văn số 548/CATTT-NCSC ngày 19/4/2022 về nguy cơ tấn công vào hệ thống thông tin của các cơ quan, tổ chức thông qua lỗ hổng bảo mật CVE 2022-29464 của Cục An toàn thông tin, Bộ Thông tin và Truyền thông. Theo đó, 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. (*Chi tiết các lỗ hổng tại Phụ lục kèm theo*).

Để tăng cường chủ động phòng ngừa các rủi ro mất an toàn thông tin tại các hệ thống thông tin của các cơ quan, địa phương do hình thức tấn công trên có thể xảy ra, Trung tâm Công nghệ thông tin và Truyền thông đề nghị các cơ quan, đơn vị chỉ đạo các bộ phận, cá nhân thực hiện những nội dung 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, các cơ quan, 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). Hướng dẫn kỹ thuật cách thức thực hiện chi tiết đối với từng lỗ hổng bảo mật tại địa chỉ:

<https://attt.thanhhoa.gov.vn>

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 quá trình thực hiện, nếu gặp khó khăn, vướng mắc về kỹ thuật liên quan đến các nội dung, công việc trên đề nghị liên hệ với Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa (cơ quan thường trực của Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh) để phối hợp hỗ trợ, xử lý.

Điện thoại: (0237)3718.699

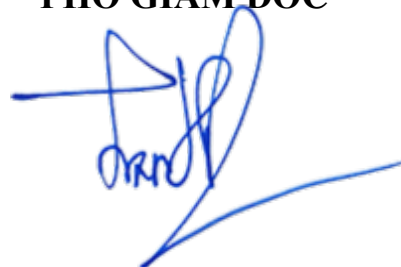
Thư điện tử: unguusuco@thanhhoa.gov.vn

Xin trân trọng cảm ơn./.

***Nơi nhận:***

- Như kính gửi;
- Sở TT&TT (để b/c);
- PGĐ Sở Nguyễn Văn Tước (để b/c);
- Giám đốc Trung tâm (để b/c);
- Lưu: VT, QTHT.

**KT. GIÁM ĐỐC  
PHÓ GIÁM ĐỐC**

A handwritten signature in blue ink, appearing to be 'Trần Ngọc Hưng', written over a horizontal line.

**Trần Ngọc Hưng**

**Phụ lục:** Thông tin các lỗ hổng bảo mật  
(Kèm theo công văn số /TTCNTT&TT-QTHT ngày tháng năm 2022  
của Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa)

---

## 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.

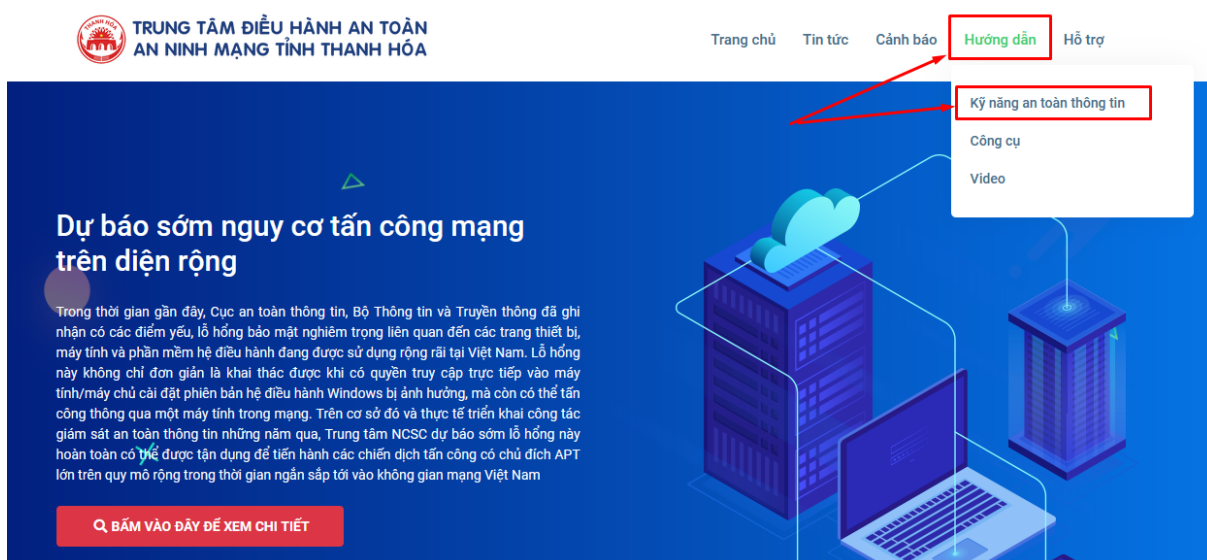
CVSS: 9.8 (Nghiêm trọng)

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

Hướng dẫn chi tiết khắc phục các lỗ hổng bảo mật trên tại địa chỉ:  
<https://attt.thanhhoa.gov.vn> (Mục Hướng dẫn → Kỹ năng An toàn thông tin)



The image shows a screenshot of the website [attt.thanhhoa.gov.vn](https://attt.thanhhoa.gov.vn). The header includes the logo of the Center for Information Security and the text "TRUNG TÂM ĐIỀU HÀNH AN TOÀN AN NINH MẠNG TỈNH THANH HÓA". The navigation menu contains "Trang chủ", "Tin tức", "Cảnh báo", "Hướng dẫn", and "Hỗ trợ". The "Hướng dẫn" menu item is highlighted with a red box, and a dropdown menu is visible with options "Kỹ năng an toàn thông tin", "Công cụ", and "Video". The "Kỹ năng an toàn thông tin" option is also highlighted with a red box. The main content area features a blue background with a server rack, a laptop, and a cloud icon. The text reads "Dự báo sớm nguy cơ tấn công mạng trên diện rộng" and provides information about the security of information system. A red button at the bottom left says "BẤM VÀO ĐÂY ĐỂ XEM CHI TIẾT".