UBND TỈNH TÂY NINH
**SỞ THÔNG TIN VÀ TRUYỀN THÔNG**

Số: 1537 /STTTT-TTGSĐH
V/v cảnh báo lỗ hổng bảo mật zero-day ảnh hưởng nghiêm trọng đến Microsoft Exchange

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

*Tây Ninh, ngày 10 tháng 10 năm 2022*

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các cơ quan tham mưu, giúp việc Tỉnh ủy;
- Mặt trận Tổ quốc và các Đoàn thể chính trị - xã hội;
- Các Sở, ban, ngành tỉnh;
- Các huyện, thị, thành ủy trực thuộc Tỉnh ủy;
- UBND các huyện, thị xã, thành phố.

Thực hiện theo Công văn số 1484/CATTT-VNCERTCC ngày 30/9/2022 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc cảnh báo lỗ hổng bảo mật zero-day ảnh hưởng nghiêm trọng đến Microsoft Exchange ***(Thông tin chi tiết phụ lục kèm theo)***.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin cho người dùng, đơn vị và toàn bộ hệ thống của tỉnh, Sở Thông tin và Truyền thông đề nghị các đơn vị, địa phương thực hiện gấp các công việc cụ thể như sau:

1. Kiểm tra xác định hệ thống phần mềm liên quan có khả năng bị ảnh hưởng. Thực hiện khắc phục kịp thời theo hướng dẫn tại phụ lục để tránh nguy cơ bị tấn công.

2. Tăng cường kiểm tra, giám sát hệ thống mạng của đơn vị, địa phương, khi có phát hiện hoạt động tấn công mạng, đề nghị liên hệ Sở Thông tin và Truyền thông để phối hợp xử lý kịp thời.

Thông tin liên quan đề nghị liên hệ Ông Vương Duy Thanh - Trung tâm Giám sát, điều hành kinh tế, xã hội tập trung; Điện thoại: 0932624462.

Trân trọng./.

***Nơi nhận:***
- Như trên;
- GĐ Sở (b/c);
- P.CNTTBCVT;
- Lưu: VT, TTGSĐH.

**KT. GIÁM ĐỐC**
**PHÓ GIÁM ĐỐC**

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TÂY NINH

**Nguyễn Trung Hiếu**

# PHỤ LỤC
## Thông tin cảnh báo lỗ hổng bảo mật zero-day ảnh hưởng nghiêm trọng đến Microsoft Exchange

### 1.Thông tin về lỗ hổng

Ngày 28/09/2022, đội ngũ bảo mật của GTSC công bố việc đang xuất hiện chiến dịch tấn công mạng có chủ đích nhắm tới các cơ quan, tổ chức trong nước thông qua việc khai thác lỗ hổng bảo mật của Microsoft Exchange.

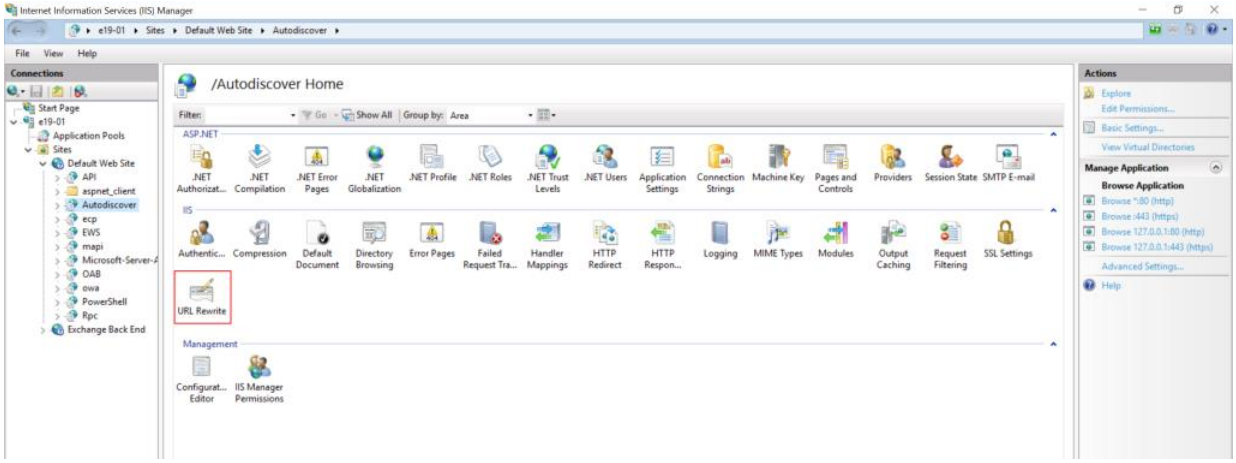
Ngày 29/9/2022, trong thông báo đăng trên blog, Microsoft cho biết họ đang điều tra hai lỗ hổng zero-day được báo cáo ảnh hưởng đến Microsoft Exchange Server 2013, 2016 và 2019. Lỗ hổng đầu tiên, được xác định là CVE-2022-41040 là lỗ hổng bảo mật SSRF, trong khi lỗ hổng thứ hai được xác định là CVE-2022-41082, cho phép thực thi mã từ xa (RCE), đây là lỗ hổng bảo mật nghiêm trọng, một khi khai thác thành công, kẻ tấn công có thể dành quyền kiểm soát toàn bộ hệ thống máy chủ Mail.

### 2. Hướng dẫn khắc phục

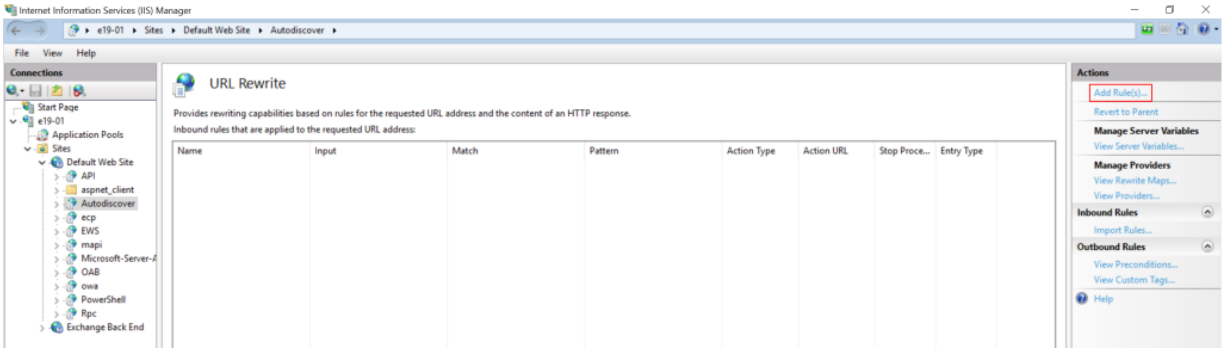
Hiện Microsoft chưa có bản vá chính thức cho lỗ hổng này, vì vậy để ngăn chặn việc khai thác lỗ hổng, đội ngũ quản trị cần cấu hình lại máy chủ theo hướng dẫn sau:

Sử dụng module URL Rewrite để chặn truy vấn khai thác lỗ hổng tại Internet Information Service (IIS) Manager

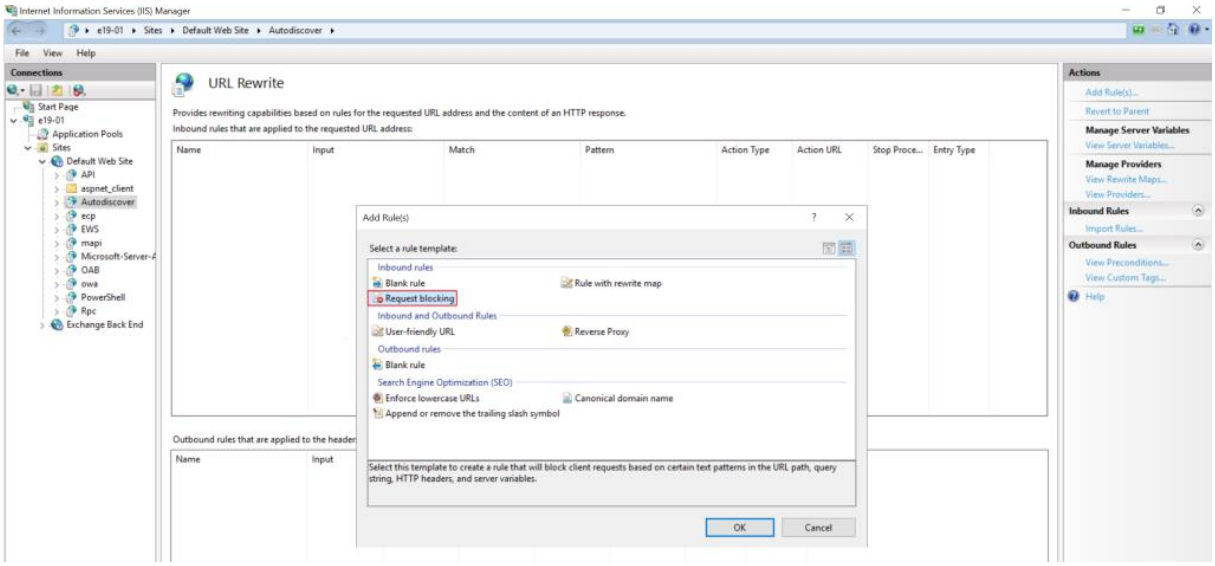
*IIS Manager -> Default Web Site -> Autodiscover -> URL Rewrite -> Actions*



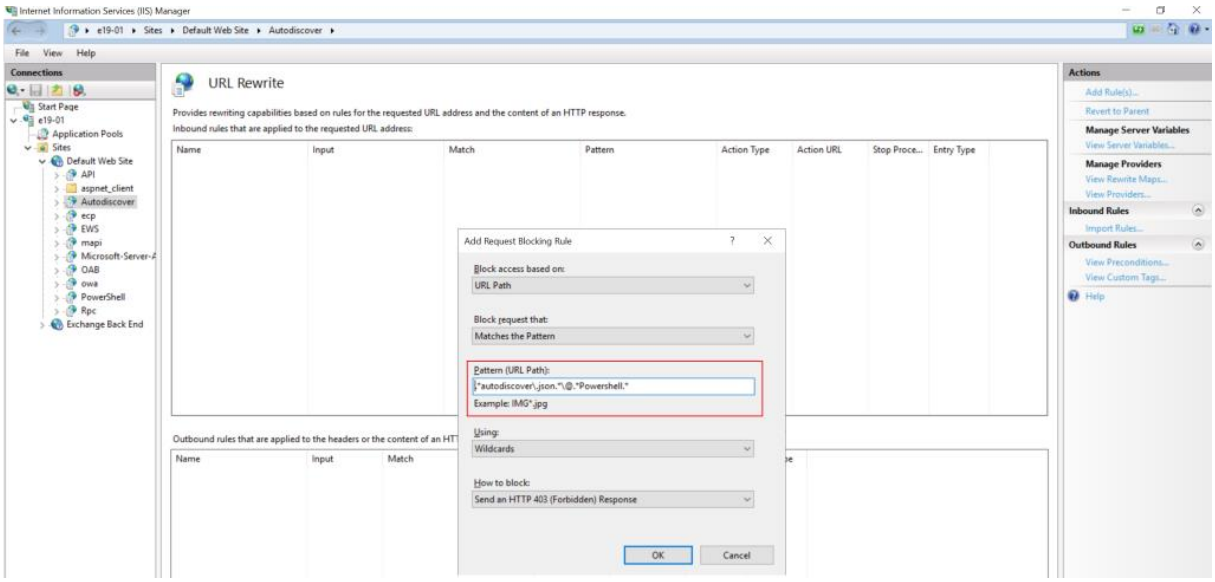

*Actions pane → click Add Rules.*



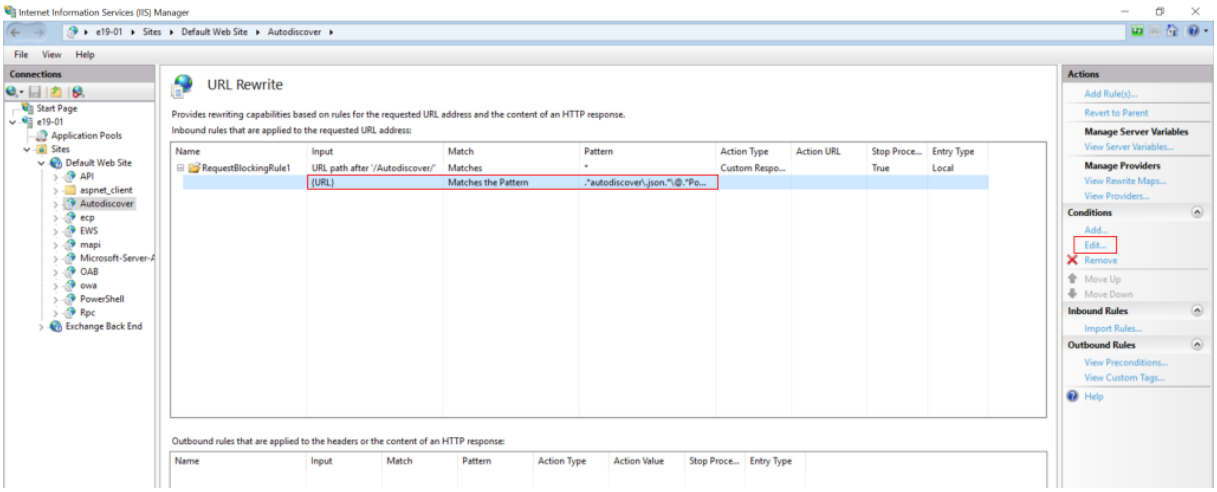

*Chọn Request Blocking và nhấn OK.*



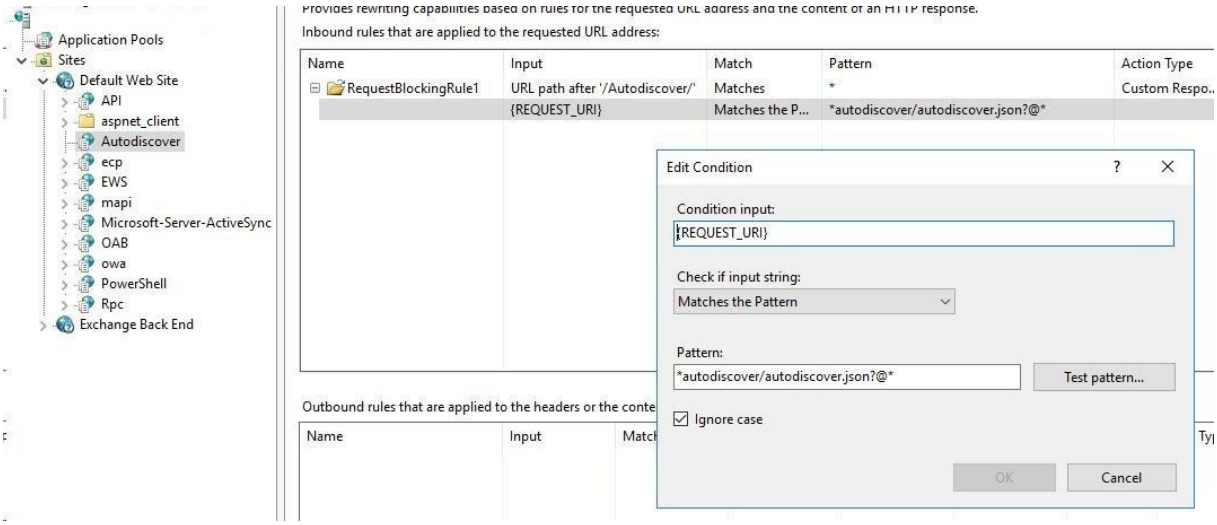

*Thêm chuỗi "*autodiscover/autodiscover.json?@*" (excluding quotes) và ấn OK.*




*Mở rộng rule và chọn the rule với chuỗi "*autodiscover/autodiscover.json?@*" sau đó nhấn Edit under Conditions.*




*Thay đổi condition input từ {URL} thành {REQUEST_URI} sau đó nhấn ok*




### 3. Công cụ hỗ trợ

- Công cụ hỗ trợ phát hiện dấu hiệu hệ thống đã bị xâm nhập: https://github.com/ncsgroupvn/NCSE0Scanner/releases

- Công cụ hỗ trợ xác nhận cấu hình thành công máy chủ để ngăn chặn tấn công: https://github.com/VNCERT-CC/0dayex-checker/releases

### 4. Liên kết tham khảo

[1]. https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server

[2]. https://www.gteltsc.vn/blog/canh-bao-chien-dich-tan-cong-su-dung-lo-hong-zero-day-tren-microsoft-exchange-server-12714.html

[3].https://www.bleepingcomputer.com/news/security/new-microsoft-exchange-zero-days-actively-exploited-in-attacks/