BỘ THÔNG TIN TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

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

Số: 1484 /CATTT-VNCERTCC

Hà Nội, ngày 30 tháng 09 năm 2022

V/v cảnh báo lỗ hổng bảo mật zero-day ảnh hưởng nghiêm trọng đến Microsoft Exchange

Kính gửi:

- Đơn vị chuyên trách về công nghệ thông tin các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước, các Ngân hàng Thương mại cổ phần, các tổ chức tài chính;
- Hệ thống các đơn vị chuyên trách về an toàn thông tin.

Thông qua việc tăng cường hợp tác, chia sẻ tri thức tấn công mạng với doanh nghiệp an toàn thông tin trong nước, Cục An toàn thông tin tiếp nhận cảnh báo từ đội ngũ bảo mật của Công ty GTSC về việc đang xuất hiện chiến dịch tấn công mạng có chủ đích sử dụng lỗ hổng zero-day, mục tiêu nhắm đến là các hệ thống máy chủ Microsoft Exchange của các cơ quan, tổ chức trong nước.

Đây là lỗ hổng bảo mật có mức độ nghiêm trọng và hiện tại chưa có bản vá lỗi chính thức, lỗ hổng này cho phép kẻ tấn công thực thi mã từ xa để dành quyền kiểm soát hệ thống, đe dọa đến tính bí mật, toàn vẹn của hàng ngàn máy chủ Mail Exchange đang được sử dụng bởi nhiều cơ quan, tổ chức trong nước *(thông tin chi tiết về lỗ hổng trong phụ lục kèm theo).*

Trước mức độ nghiêm trọng của lỗ hổng, ngày 29/9/2022, Cục An toàn thông tin đã tiến hành rà soát và ghi nhận hệ thống máy chủ Mail một số đơn vị đã bị xâm nhập với các dấu hiệu nhận diện liên quan đến tấn công có chủ đích. Đồng thời, Cục An toàn thông tin đã phát đi cảnh báo tới toàn bộ thành viên thuộc Mạng lưới ứng cứu sự cố an toàn thông tin mạng Việt Nam. Tuy nhiên, việc tuân theo khuyến nghị để ngăn chặn việc khai thác lỗ hổng vẫn chưa được thực hiện nghiêm túc.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị,

góp phần bảo đảm an toàn không gian mạng Việt Nam, Cục An toàn thông tin đề nghị Quý đơn vị thực hiện:

1. Cấu hình lại máy chủ để ngăn chặn đối tượng tấn công thực thi mã từ xa *(chi tiết hướng dẫn trong phụ lục kèm theo)*.

2. Sử dụng công cụ thực hiện rà soát lại hệ thống máy chủ Mail và công cụ kiểm tra cấu hình ngăn chặn tấn công để phát hiện các dấu hiệu bị xâm nhập và tính hiệu của của biện pháp ngăn chặn nhằm kịp thời ứng phó trước khi sự cố xảy ra *(công cụ gửi kèm theo)*.

3. 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 https://t.me/+TEXoMVQDhNoyMDI1 để cập nhật kịp thời các nguy cơ, chiến dịch tấn công mạng.

Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam; điện thoại 0869100317; thư điện tử: ir@vncert.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Huy Dũng (để b/c);
- Cục A05, Bộ Công an (để biết);
- Bộ Tư lệnh 86, Bộ Quốc phòng (để biết);
- Ban Cơ yếu Chính phủ (để biết);
- Cục trưởng (để b/c);
- PCT Trần Đăng Khoa;
- Trung tâm NCSC, phòng ATHTTT;
- Lưu: VT, VNCERT/CC.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Trần Đăng Khoa

Phụ lục

Thông tin về lỗ hổng bảo mật trong sản phẩm Microsoft Exchange

(Kèm theo Công văn số /CATTT-VNCERTCC ngày / /2022 của Cục An toàn thông tin)

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.

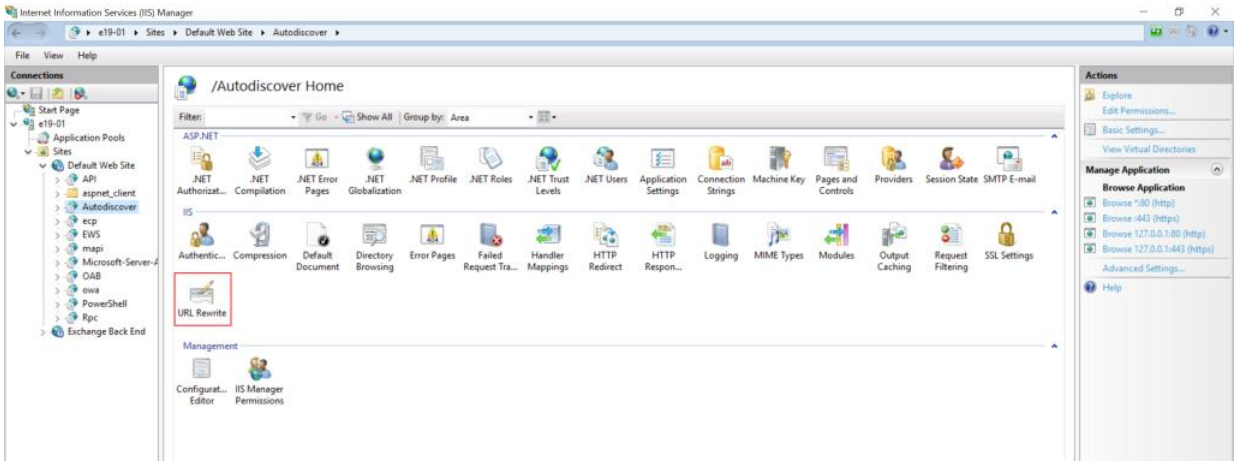
Ngày 29/9/2022, trong thông báo đăng trên blog, Microsoft cho biết họ đang điều tra hai lỗ hổng zero-day được báo cáo ảnh hưởng đến Microsoft Exchange Server 2013, 2016 và 2019. Lỗ hổng đầu tiên, được xác định là CVE-2022-41040 là lỗ hổng bảo mật SSRF, trong khi lỗ hổng thứ hai được xác định là CVE-2022-41082, 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

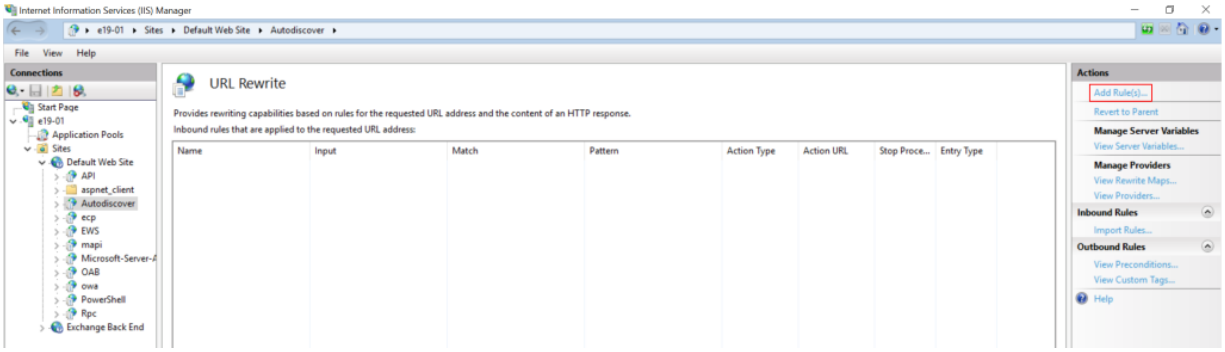
Hiện Microsoft chưa có bản vá chính thức cho lỗ hổng này, vì vậy để ngăn chặn việc khai thác lỗ hổng, đội ngũ quản trị cần cấu hình lại máy chủ theo hướng dẫn sau:

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

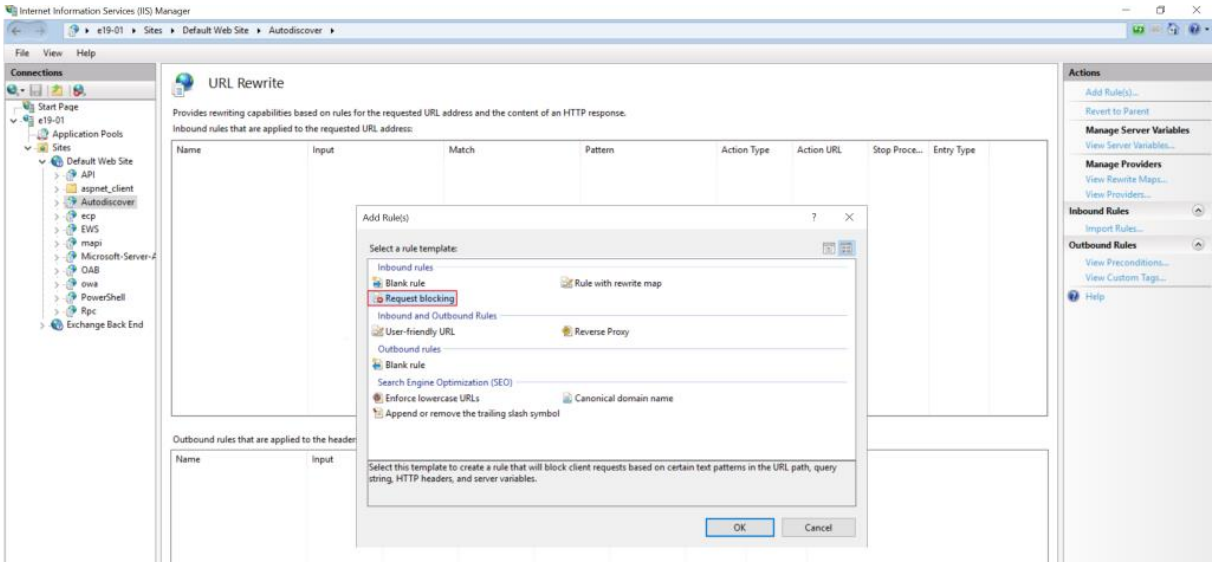
IIS Manager -> Default Web Site -> Autodiscover -> URL Rewrite -> Actions



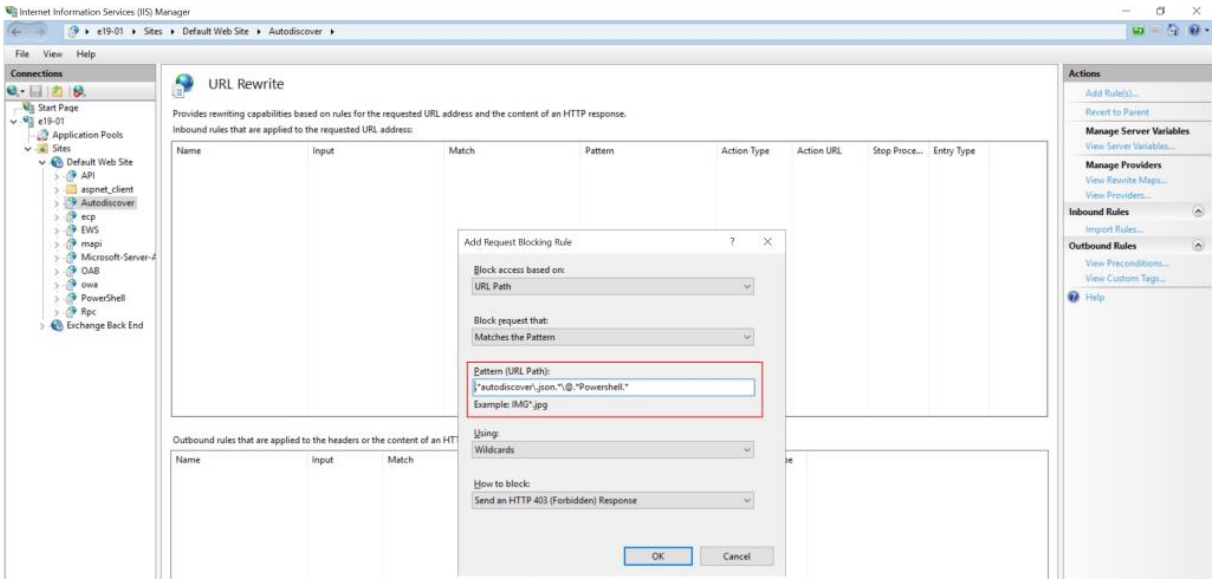
Actions pane → click Add Rules.



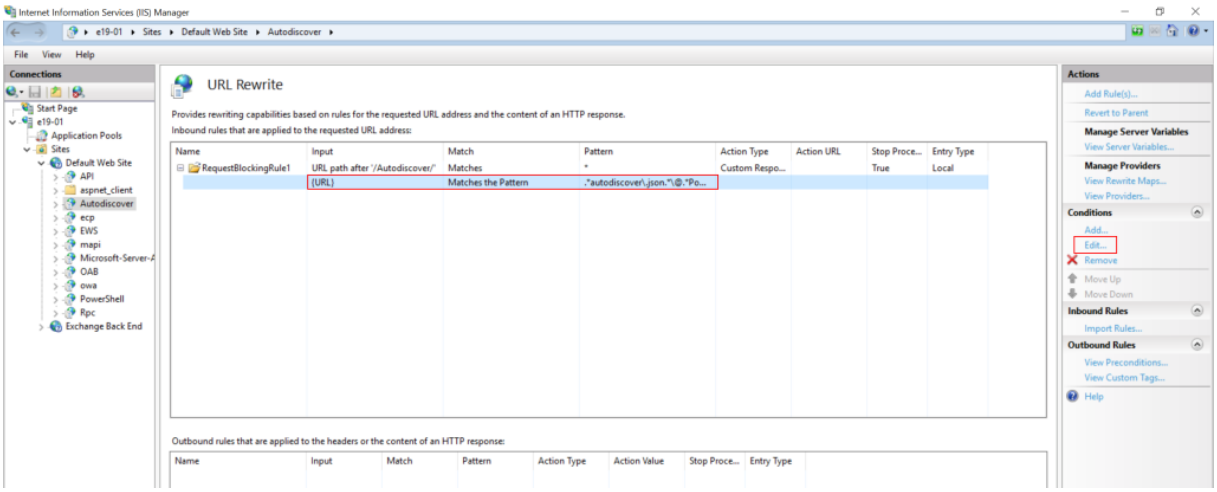
Chọn Request Blocking và nhấn OK.



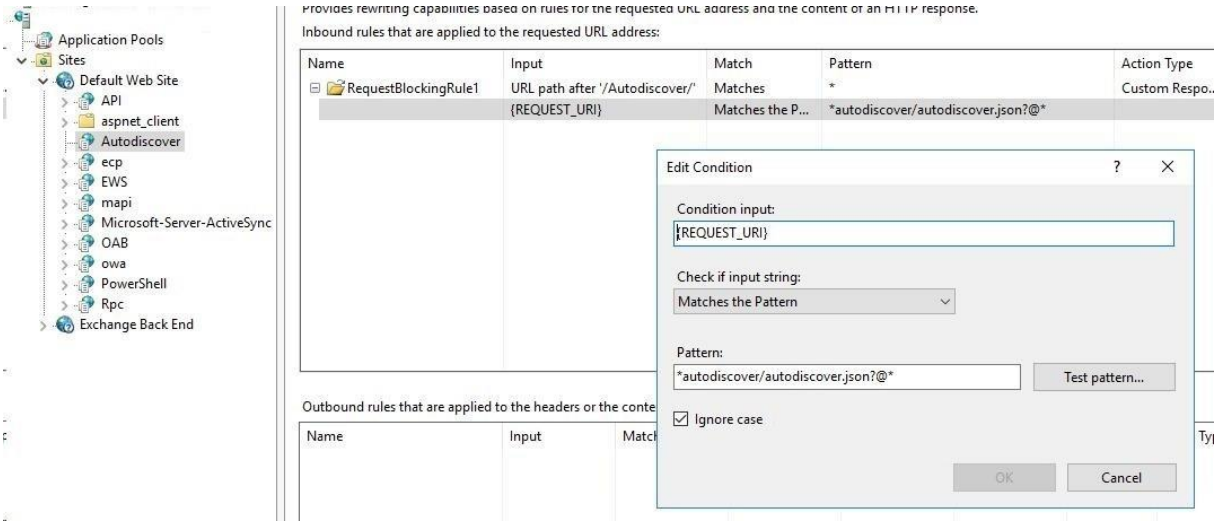
*Thêm chuỗi "*autodiscover/autodiscover.json?@*" (excluding quotes) và ấn OK.*



*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/