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.

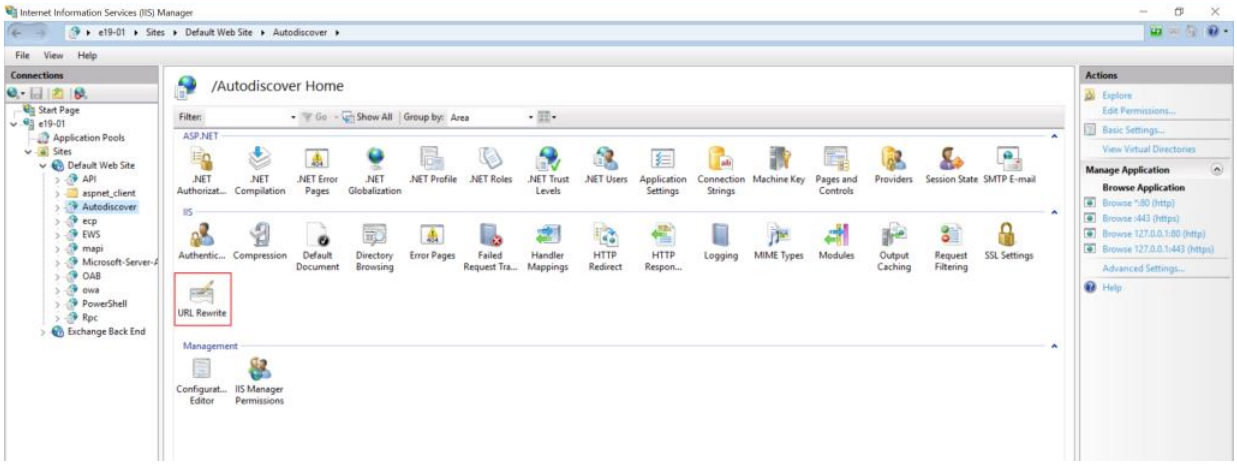
Ngày 29/9/2022, trong thông báo đăng trên blog, Microsoft cho biết họ đang điều tra hai lỗ hổng zero-day được báo cáo ảnh hưởng đến Microsoft Exchange Server 2013, 2016 và 2019. Lỗ hổng đầu tiên, được xác định là CVE-2022-41040 là lỗ hổng bảo mật SSRF, trong khi lỗ hổng thứ hai được xác định là CVE-2022-41082,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

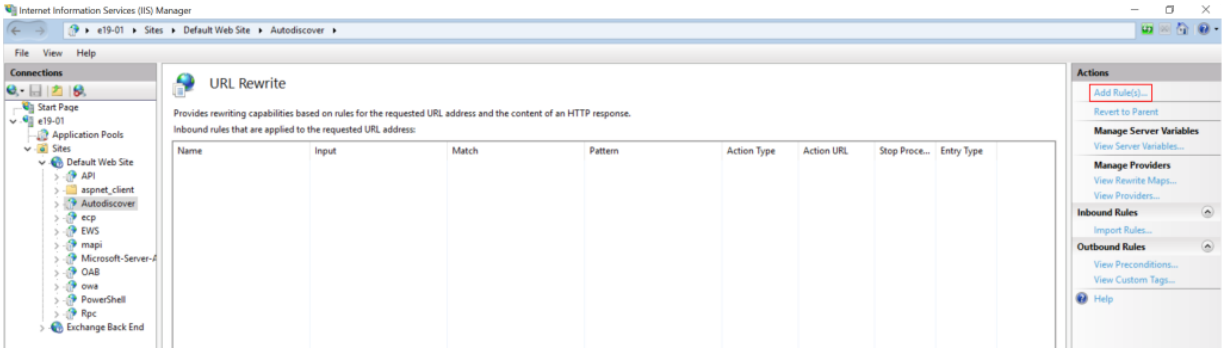
Hiện Microsoft chưa có bản vá chính thức cho lỗ hổng này, vì vậy để ngăn chặn việc khai thác lỗ hổng, đội ngũ quản trị cần cấu hình lại máy chủ theo hướng dẫn sau:

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

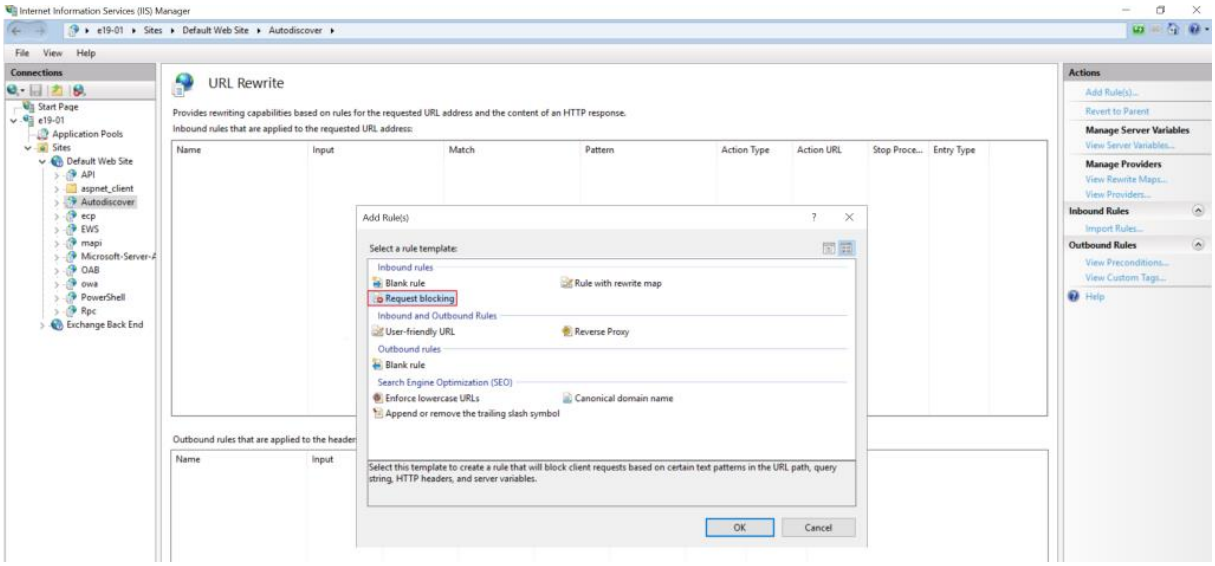
IIS Manager -> Default Web Site -> Autodiscover -> URL Rewrite -> Actions



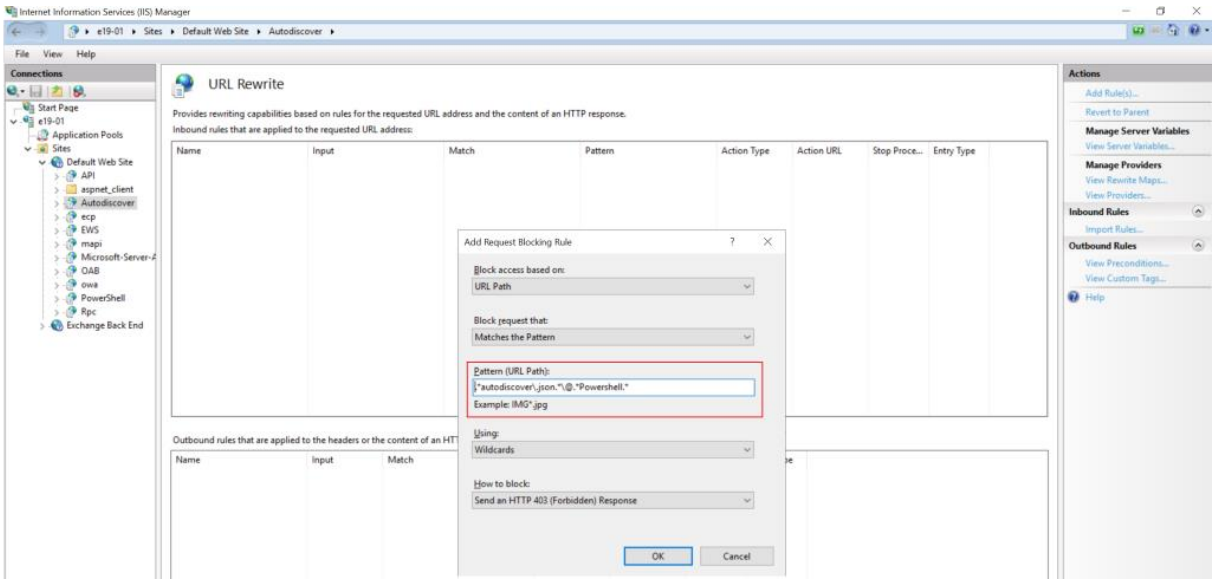
Actions pane → click Add Rules.



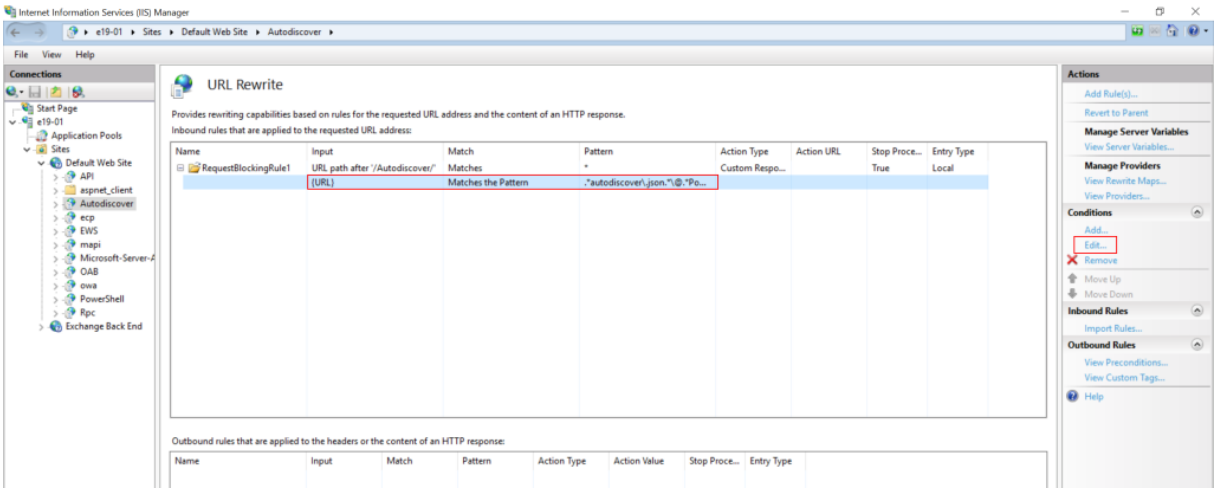
Chọn Request Blocking và nhấn OK.



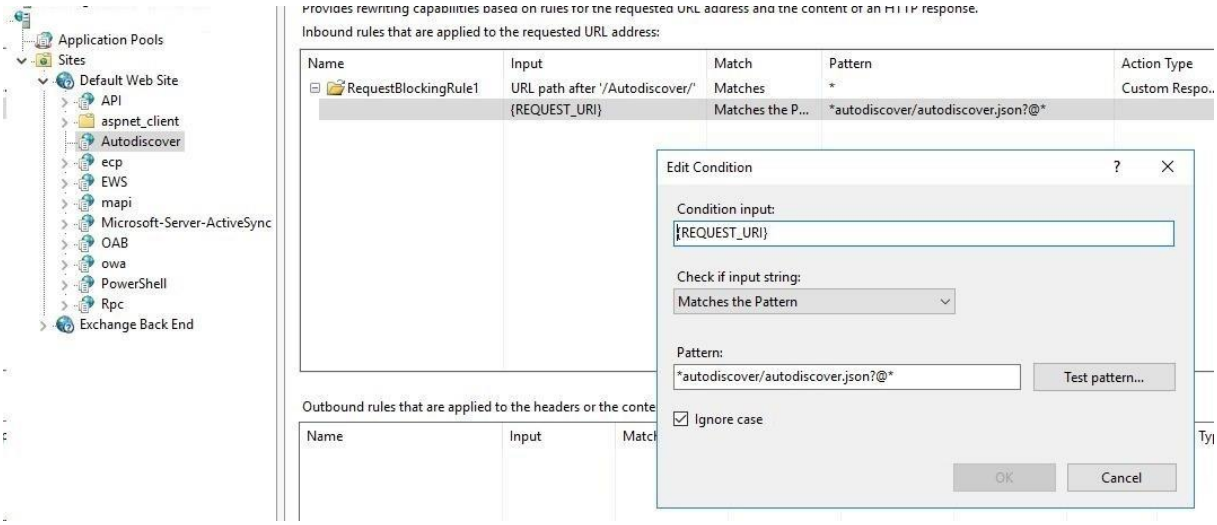
*Thêm chuỗi "*autodiscover/autodiscover.json?@*" (excluding quotes) và ấn OK.*



*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/