BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

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

Số: 88 /TTCNTT-KTHT
V/v 04 lỗ hổng bảo mật mới ảnh hưởng nghiêm trọng tới máy chủ thư điện tử Microsoft Exchange Server và hướng dẫn xử lý

Hà Nội, ngày 20 tháng 04 năm 2021

Kính gửi: Các đơn vị trực thuộc Bộ có hệ thống công nghệ thông tin

Thư điện tử (email) là công cụ trao đổi thông tin, công việc được hầu hết các cơ quan tổ chức sử dụng. Tại Việt Nam, Microsoft Exchange Server là một trong những phần mềm được sử dụng phổ biến nhất để quản lý hệ thống thư điện tử. Đặc biệt khi tình hình đại dịch COVID-19 đang diễn ra phức tạp, thì việc trao đổi công việc trực tuyến thông qua email ngày càng được sử dụng nhiều hơn. Do vậy, công cụ này hiện nay là mục tiêu hàng đầu mà đối tượng tấn công nhằm đến để đánh cắp thông tin nhạy cảm. Trong trường hợp khai thác thành công các hệ thống email, đối tượng tấn công không chỉ kiểm soát được toàn bộ hệ thống thư điện tử mà từ đó có thể sử dụng làm bàn đạp để tấn công các hệ thống thông tin quan trọng khác của cơ quan, tổ chức.

Theo đánh giá sơ bộ của Cục An toàn thông tin – Bộ Thông tin và Truyền thông, rất nhiều hệ thống thư điện tử của Việt Nam (như máy chủ thư điện tử của cơ quan tổ chức nhà nước, tổ chức ngân hàng, tài chính, các doanh nghiệp và các tổ chức lớn khác) đang sử dụng Microsoft Exchange Server. Tại Việt Nam có khoảng hơn 500 hệ thống đang sử dụng Microsoft Exchange Server (trong đó có nhiều hệ thống thuộc Cơ quan Nhà nước). Các hệ thống này là mục tiêu chính của các nhóm đối tượng tấn công mạng có chủ đích (APT), do đó nguy cơ bị tấn công là rất cao khi xuất hiện lỗ hổng bảo mật mới trong Microsoft Exchange Server.

Tháng 03/2021, Trung tâm Công nghệ thông tin (Trung tâm CNTT) đã cảnh báo tới các Quý đơn vị về các lỗ hổng bảo mật **(CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065)** ảnh hưởng đến Microsoft Exchange Server. Đầu tháng 04/2021, Trung tâm CNTT tiếp tục ghi nhận thông tin về 04 lỗ hổng mới **(CVE-2021-28480, CVE-2021-28481, CVE-2021-28482, CVE-2021-28483)** ảnh hưởng nghiêm trọng đến Microsoft Exchange Server, cho phép đối tượng tấn công chèn và thực thi lệnh độc hại, cài cắm mã độc và chiếm điều khiển hệ thống. Trong đó:

- 02 lỗ hổng CVE-2021-28480 và CVE-2021-28481: có thể sử dụng để tấn công vào hệ thống mà không cần có tài khoản đăng nhập hợp lệ. Các lỗ hổng này tương tự như CVE-2021-26855 (ProxyLogon) đã được cảnh báo trước đó.

- 02 lỗ hổng CVE-2021-28482 và CVE-2021-28483: để khai thác đối tượng

tấn công cần xác thực vào hệ thống Exchange Server.

Các lỗ hổng bảo mật này có thể đã, đang và sẽ được các nhóm tấn công APT sử dụng để khai thác trong thời gian ngắn sắp tới. Nhằm bảo đảm an toàn thông tin cho hệ thống thông tin của Quý đơn vị, Trung tâm CNTT yêu cầu Quý đơn vị chỉ đạo thực hiện:

1. Kiểm tra, xác minh hệ thống thông tin có khả năng bị ảnh hưởng bởi lỗ hổng trên để có phương án xử lý, khắc phục lỗ hổng, tham khảo hướng dẫn tại phụ lục kèm theo; đồng thời nên thực hiện rà soát và xử lý các vấn đề an toàn thông tin cho hệ thống thư điện tử.

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đặc biệt tiến hành rà soát lại toàn bộ hệ thống máy chủ thư điện tử và các hệ thống thông tin liên quan khác để có biện pháp xử lý kịp thời trong trường hợp bị tấn công.

3. Đề nghị các Quý đơn vị gửi thông tin kết quả hoàn thành việc khắc phục lỗ hổng bảo mật nói trên về đầu mối hỗ trợ của Trung tâm Công nghệ thông tin: Phòng Kỹ thuật hạ tầng, điện thoại 024.39439060, thư điện tử: phongktht@most.gov.vn.

Trân trọng./

Nơi nhận:
- Như trên;
- Thứ trưởng Bùi Thế Duy (để b/c);
- Cổng thông tin điện tử Bộ KH&CN;
- Lưu: VT, KTHT.

GIÁM ĐỐC

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Hà Quốc Trung

Phụ lục
Thông tin về các lỗ hổng bảo mật trong Microsoft Exchange Server
(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2021)

1. Thông tin các lỗ hổng bảo mật

TT	CVE	Mô tả	Link tham khảo hướng dẫn
1	CVE-2021-28480	Điểm CVSS: 9.8 (nghiêm trọng) Cho phép đối tượng tấn công không cần tài khoản xác thực để thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-28480
2	CVE-2021-28481	Điểm CVSS: 9.8 (nghiêm trọng) Cho phép đối tượng tấn công không cần tài khoản xác thực đế thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-28481
3	CVE-2021-28482	Điểm CVSS: 8.8 (cao) Cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-28482
4	CVE-2021-28483	Điểm CVSS: 9.0 (cao) Cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-28483

2. Hướng dẫn khắc phục

Đối với các tổ chức không áp dụng được các bản vá cho các lỗ hổng Exchange Server trước đó thì cần update các bản vá này (chúng có thể khắc phục được cả 08 lỗ hổng mà Microsoft đã vá kể từ ngày 03 tháng 03 vừa qua).

04 lỗ hổng này khác với các lỗ hổng trước. Do đó, việc chạy các công cụ và tập lệnh bảo mật vào tháng 03 năm 2021 theo Microsoft sẽ không giảm thiểu hay khắc phục được các lỗ hổng bảo mật này.

Tại thời điểm này không có các biện pháp khắc phục giảm thiểu thay thế cho các lỗ hổng bảo mật nói trên. Vì vậy các đơn vị cần cập nhật máy chủ của mình càng sớm càng tốt. Trong trường hợp có các biện pháp thay thế khắc phục khác từ Microsoft, Trung tâm CNTT sẽ cập nhập trong thời gian tới.

2.1. Thông tin các phiên bản ảnh hưởng và bản vá tương ứng:

TT	Phiên bản ảnh hưởng	Bản cập nhật
1	Exchange Server 2013 CU 23	https://www.microsoft.com/en-us/download/details.aspx?id=103000
2	Exchange Server 2016 CU 20	https://www.microsoft.com/en-us/download/details.aspx?id=103002
3	Exchange Server 2016 CU 19	https://www.microsoft.com/en-us/download/details.aspx?id=103001
4	Exchange Server 2019 CU 9	https://www.microsoft.com/en-us/download/details.aspx?id=103004
5	Exchange Server 2019 CU 8	https://www.microsoft.com/en-us/download/details.aspx?id=103003

Ghi chú: Trong một số trường hợp cài đặt thủ công bản cập nhật bảo mật này bằng cách nhấn đúp vào tệp cập nhật (.msp) để chạy ở chế độ bình thường, một số tệp tin không được cập nhật chính xác. Lúc này, các quản trị viên sẽ không nhận được thông báo lỗi hoặc bất kỳ dấu hiệu nào cho thấy bản cập nhật bảo mật không được cài đặt đúng cách. Tuy nhiên, Outlook Web Access (OWA) và Exchange Control Panel (ECP) có thể sẽ ngừng hoạt động.

2.2. Các bước cập nhật (nên tắt phần mềm anti-virus trước khi thực hiện cập nhật)

Mở cửa sổ nâng cao Command Prompt (không phải PowerShell) với quyền admin:

Bước 1: Chọn Start/cmd

Bước 2: Chuột phải vào Command Prompt và chọn Run as administrator.

Bước 3: Hộp thoại User Account Control xuất hiện, chọn Yes/Next.

Bước 4: Nhập đường dẫn đầy đủ đã tải về đến thư mục chứa “MSP file” và nhấn Enter (chú ý không bấm đúp vào “MSP file’ để chạy)

Khi quá trình cài đặt hoàn tất, hãy bật lại phần mềm anti-virus và khởi động lại máy.

DANH SÁCH CÁC ĐƠN VỊ CÓ HỆ THỐNG CNTT

(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2021)

STT	Tên đơn vị
1	Cục Thông tin khoa học và công nghệ quốc gia
2	Cục Sở hữu trí tuệ
3	Tổng cục Tiêu chuẩn Đo lường Chất lượng
4	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo
5	Viện Năng lượng nguyên tử Việt Nam
6	Viện Khoa học sở hữu trí tuệ
7	Quỹ phát triển khoa học và công nghệ quốc gia
8	Cục An toàn bức xạ và hạt nhân
9	Quỹ đổi mới công nghệ quốc gia
10	Ban Quản lý Khu công nghệ cao Hòa Lạc