UBND TỈNH GIA LAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 633/STTTT-CNTT
V/v cảnh báo 04 lỗ hổng bảo mật mới ảnh hưởng nghiêm trọng tới máy chủ thư điện tử Microsoft Exchange Server

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

Gia Lai, ngày 05 tháng 5 năm 2021

Kính gửi:

- Công an tỉnh;
- Bộ Chỉ huy Quân sự tỉnh;
- Bộ Chỉ huy Bộ đội biên phòng tỉnh;
- Văn phòng Tỉnh ủy;
- Văn phòng Hội đồng nhân dân tỉnh;
- Văn phòng Ủy ban Mặt trận tổ quốc Việt Nam tỉnh;
- Các sở, ban, ngành thuộc tỉnh;
- Các hội, đoàn thể tỉnh;
- Ủy ban nhân dân các huyện, thị xã, thành phố;
- Trung tâm CNTT&TT tỉnh Gia Lai.

Theo đánh giá của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) thuộc 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 Giám sát an toàn không gian mạng quốc gia đã thực hiện cảnh báo rộng rãi tới các cơ quan, tổ chức, doanh nghiệp về các lỗ hổng bảo mật (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065) ảnh hưởng đến Microsoft Exchange Server. Nhiều cơ quan, tổ chức đã phản hồi thông tin thực hiện khắc phục, xử lý các lỗ hổng trên theo hướng dẫn của NCSC.

Đầu tháng 04/2021, Trung tâm NCSC 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 quyền 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.

- 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.

Thực hiện chỉ đạo của Ủy ban nhân dân tỉnh Gia Lai tại Công văn số 1623/VP-KGVX ngày 23/4/2021 về việc cảnh báo 04 lỗ hổng bảo mật mới ảnh hưởng nghiêm trọng tới máy chủ thư điện tử Microsoft Exchange Server và hướng dẫn xử lý; Sở Thông tin và Truyền thông tỉnh Gia Lai đề nghị các đơn vị, địa phương có sử dụng hệ thống thư điện tử Microsoft Exchange kiểm tra, khắc phục kịp thời các lỗ hổng bảo mật ảnh hưởng nghiêm trọng tới máy chủ thư điện tử Microsoft Exchange Server, cụ thể như sau:

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 (*hướng dẫn chi tiết trong Phụ lục đính kèm*); 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. Gửi thông tin kết quả hoàn thành việc khắc phục lỗ hổng bảo mật nói trên về Sở Thông tin và Truyền thông tỉnh Gia Lai trước ngày **11/5/2021**, để tổng hợp, báo cáo Ủy ban nhân dân tỉnh Gia Lai.

Sở Thông tin và Truyền thông tỉnh Gia Lai đề nghị các đơn vị, địa phương phối hợp, triển khai thực hiện./.

Nơi nhận:
- Như trên;
- UBND tỉnh (báo cáo);
- Lưu: VT, P. CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Đặng Quang Khanh

Phụ lục:

THÔNG TIN VỀ 04 LỖ HỔNG BẢO MẬT MỚI ẢNH HƯỞNG NGHIÊM TRỌNG TỚI MÁY CHỦ THƯ ĐIỆN TỬ MICROSOFT EXCHANGE SERVER VÀ HƯỚNG DẪN XỬ LÝ, KHẮC PHỤC LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số : 633/STTTT-CNTT ngày 05 tháng 4/2021 của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng bảo mật

Số TT	Tên lỗ hổng	Mô tả	Link tham khảo hướng dẫn
1	CVE-2021-28480	Cho phép đối tượng tấn công không cần tài khoản xác thực để thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/enUS/vulnerability/CVE-2021-28480
2	CVE-2021-28481	Cho phép đối tượng tấn công không cần tài khoản xác thực để thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/enUS/vulnerability/CVE-2021-28481
3	CVE-2021-28482	Cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/enUS/vulnerability/CVE-2021-28482
4	CVE-2021-28483	Cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/enUS/vulnerability/CVE-2021-28483

2. Hướng dẫn khắc phục

2.1 Thông tin các phiên bản ảnh hưởng và bản vá lỗi

Số TT	Phiên bản ảnh hưởng	Bản cập nhật
1	Exchange Server 2013 CU 23	https://www.microsoft.com/enus/download/details.aspx?id=103000
2	Exchange Server 2016 CU 20	https://www.microsoft.com/enus/download/details.aspx?id=103002
3	Exchange Server 2016 CU 19	https://www.microsoft.com/enus/download/details.aspx?id=103001

4	Exchange Server 2019 CU 9	https://www.microsoft.com/enus/download/details.aspx?id=103004
5	Exchange Server 2019 CU 8	https://www.microsoft.com/enus/download/details.aspx?id=103003

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 chủ.