UBND TỈNH GIA LAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 427/STTTT-CNTT
V/v hoạt động tấn công mạng, khai thác lỗ hổng bảo mật của phần mềm Microsoft Exchange

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

Gia Lai, ngày 26 tháng 3 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.

Theo công bố của hãng Microsoft ngày 02/3/2021, các máy chủ thư điện tử sử dụng phần mềm Microsoft Exchange với các phiên bản 2013, 2016 và 2019 có 04 lỗ hổng bảo mật zero-day ở mức độ đặc biệt nghiêm trọng (mã lỗi CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065). Lợi dụng các mã lỗi này tin tặc có thể thực thi các lệnh điều khiển từ xa, qua đó cài đặt các loại mã độc để kiểm soát máy chủ, tải xuống thư điện tử của người dùng mà không cần xác thực; mở rộng leo thang tấn công kiểm soát hệ thống mạng.

Mặc dù hãng Microsoft đã phát hành bản cập nhật cho phần mềm Microsoft Exchange, tuy nhiên, việc cập nhật bản vá bảo mật của hãng Microsoft chỉ khắc phục được lỗ hổng bảo mật đã được công bố nhưng không gỡ bỏ được các chương trình, mã độc gián điệp đã được cài trên máy chủ trong hệ thống mạng. Nếu không xử lý, ngăn chặn kịp thời sẽ dẫn đến nguy cơ mất an toàn, an ninh mạng, lộ, mất tài liệu nội bộ, bí mật nhà nước.

Để bảo đảm an toàn, an ninh mạng và phòng, chống lộ, mất bí mật nhà nước, Sở Thông tin và Truyền thông đề nghị các đơn vị, địa phương khẩn trương, rà soát, kiểm tra, khắc phục kịp thời lỗ hổng bảo mật trên các máy chủ thư điện tử sử dụng phần mềm Microsoft Exchange, cụ thể như sau:

1. Rà soát, kiểm tra lại các máy chủ thư điện tử có sử dụng phần mềm Microsoft Exchange với các phiên bản 2013, 2016 và 2019.

2. Cập nhật bản vá bảo mật của hãng Microsoft, khắc phục lỗ hổng bảo mật *(hướng dẫn chi tiết trong Phụ lục đính kèm).*

3. Tăng cường công tác giám sát an toàn, an ninh mạng cho hệ thống thông tin trong cơ quan hành chính nhà nước; rà soát, loại bỏ các chương trình, mã độc gián điệp đã được cài trên máy chủ trong hệ thống mạng.

4. Chấp hành nghiêm chỉnh các quy định của pháp luật về bảo vệ bí mật nhà nước; không lưu trữ, truyền đưa tài liệu bí mật nhà nước qua thư điện tử nếu không áp dụng các giải pháp mã hóa dữ liệu.

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

Nơi nhận:
- Như trên;
- UBND tỉnh (báo cáo);
- Trung tâm CNTT&TT tỉnh Gia Lai;
- Lưu: VT, P. CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Đặng Quang Khanh

Phụ lục:

CHI TIẾT KHẮC PHỤC

LỖ HỔNG BẢO MẬT CỦA MICROSOFT EXCHANGE

(Kèm theo Công văn số : /STTTT-CNTT ngày tháng 3/2021 của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng bảo mật:

Số TT	Tên lỗ hổng	Mô tả	Hướng dẫn vá lỗ hổng
1	CVE-2021-26855	Cho phép đối tượng thực hiện tấn công SSRF	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26855
2	CVE-2021-26857	Lỗi insecure deserialization, cho phép đối tượng tấn công thực thi mã với quyền hệ thống.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26857
3	CVE-2021-26858	Cho phép đối tượng tấn công ghi file tùy ý sau xác thực.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26858
4	CVE-2021-27065	Cho phép đối tượng tấn công ghi file tùy ý sau xác thực.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27065

2. Thông tin các phiên bản ảnh hưởng và bản vá lỗi:

Số TT	Phiên bản ảnh hưởng	Bản cập nhật
1	Exchange Server 2013	https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-march-2-2021-kb5000871-9800a6bb-0a21-4ee7-b9da-fa85b3e1d23b
2	Exchange Server 2016	https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-march-2-2021-kb5000871-9800a6bb-0a21-4ee7-b9da-fa85b3e1d23b
3	Exchange Server 2019	https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-march-2-2021-kb5000871-9800a6bb-0a21-4ee7-b9da-fa85b3e1d23b