UBND TỈNH GIA LAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 1842/STTTT-CNTT
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 10/2023

Gia Lai, ngày 20 tháng 10 năm 2023

Kính gửi:

- Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh Gia Lai;
- Công an tỉnh Gia Lai;
- Bộ Chỉ huy Quân sự tỉnh;
- Bộ Chỉ huy Bộ đội biên phòng tỉnh;
- Văn phòng Đoàn đại biểu Quốc hội và Hội đồng nhân dân tỉnh;
- Các Sở, ban, ngành thuộc tỉnh;
- Các hội, đoàn thể của tỉnh;
- Ủy ban nhân dân các huyện, thị xã, thành phố;
- Trung tâm CNTT&TT tỉnh Gia Lai;
- Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh Gia Lai *(Theo Quyết định số: 112/QĐ-ĐUCSCATTTM ngày 31/8/2023 của Đội trưởng Đội ƯCSCATTTM tỉnh Gia Lai).*

Ngày 10/10/2023, Microsoft đã phát hành danh sách bản vá tháng 10 với 103 lỗ hổng bảo mật trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý các lỗ hổng bảo mật có mức ảnh hưởng cao và nghiêm trọng sau:

- Lỗ hổng an toàn thông tin **CVE-2023-36778** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.

Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin (Bộ Thông tin và Truyền thông), đã phát hành các văn bản cảnh báo diện rộng về những lỗ hổng ảnh hưởng đến Microsoft Exchange Server (*nội dung này Sở Thông tin và Truyền thông đã gửi công văn cho các đơn vị để tự kiểm tra, rà soát*). Điều này cho thấy Microsoft Exchange Server vẫn luôn là mục tiêu hàng đầu được các đối tượng tấn công có chủ đích nhắm đến. Vì vậy, để đảm bảo an toàn thông tin cho hệ thống của đơn vị, Sở Thông tin và Truyền thông đề nghị các đơn vị chủ động tự rà soát lỗ hổng liên quan đến Microsoft Exchange Server để phát hiện và có phương án xử lý kịp thời, đồng thời tăng cường giám sát nhằm giảm thiểu nguy cơ bị tấn công thông qua các lỗ hổng này.

- Lỗ hổng an toàn thông tin **CVE-2023-36563** trong Microsoft WordPad cho phép đối tượng tấn công thực hiện thu thập thông tin mã băm NTLM của người dùng. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2023-41763** trong Skype for Business cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

- 02 lỗ hổng an toàn thông tin **CVE-2023-35349, CVE-2023-36697** trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2023-36434** trong Windows IIS Server cho phép đối tượng tấn công thực hiện leo thang đặc quyền.

Thực hiện khuyến nghị của Cục An toàn thông tin (Bộ Thông tin và Truyền thông) tại Công văn số 1850/CATTT-NCSC ngày 19/10/2023 về việc "lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 10/2023"; Sở Thông tin và Truyền thông đề nghị các đơn vị, địa phương kiểm tra, rà soát, khắc phục kịp thời lỗ hổng bảo mật ảnh hưởng mức cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 10/2023, cụ thể như sau:

1. Kiểm tra, rà soát, xác định máy sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng bởi lỗ hổng bảo mật trên để có phương án xử lý, khắc phục. Thực hiện cập nhật bản vá kịp thời cho các lỗ hổng bảo mật để tránh nguy cơ bị tấn công (*Hướng dẫn chi tiết tại Phụ lục đính kèm*).

2. 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 của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

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);
- Cục An toàn thông tin (Bộ TT&TT);
- Văn phòng Tỉnh ủy;
- Lưu: VT, P. CNTT.

GIÁM ĐỐC

CỘNG HÒA X H C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH GIA LAI

Nguyễn Ngọc Hùng

Phụ lục:

THÔNG TIN VỀ LỖ HỔNG BẢO MẬT ẢNH HƯỞNG MỨC CAO VÀ NGHIÊM TRỌNG TRONG CÁC SẢN PHẨM MICROSOFT CÔNG BỐ THÁNG 10/2023 VÀ HƯỚNG DẪN XỬ LÝ, KHẮC PHỤC LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số: 1842/STTTT-CNTT ngày 20 tháng 10 năm 2023 của Sở Thông tin và Truyền thông tỉnh Gia Lai)

1. Thông tin các lỗ hổng bảo mật:

Số TT	CVE	Mô tả	Link tham khảo
1	CVE-2023-36778	- Điểm: CVSS: 8.0 (Cao) - Mô tả: Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Exchange Server 2016, 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36778
2	CVE-2023-36563	- Điểm: CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng trong Microsoft WordPad cho phép đối tượng tấn công thực hiện thu thập thông tin mã băm NTLM của người dùng. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36563
3	CVE-2023-41763	- Điểm: CVSS: 5.3 (Cao) - Mô tả: Lỗ hổng trong Skype for Business cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng:	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-41763

Số TT	CVE	Mô tả	Link tham khảo
		Skype for Business 2015, 2019.	
4	CVE-2023-35349 CVE-2023-36697	- Điểm: CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35349 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36697
5	CVE-2023-36434	- Điểm: CVSS: 9.8 (Cao) - Mô tả: Lỗ hổng trong Windows IIS Server cho phép đối tượng tấn công thực hiện leo thang đặc quyền. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36434

2. Hướng dẫn khắc phục:

Thực hiện cập nhật bản vá cho các lỗ hổng bảo mật nói trên theo hướng dẫn của hãng Microsoft. Các đơn vị tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại link nguồn tham khảo tại mục 1 của Phụ lục.

3. Tài liệu tham khảo:

- https://msrc.microsoft.com/update-guide/
- https://www.zerodayinitiative.com/blog/2023/10/10/the-october-2023-security-update-review