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: 1648/STTTT-CNTT
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 9/2023

Gia Lai, ngày 26 tháng 9 năm 2023

Kính gửi:

- Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh;
- 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.

Ngày 12/9/2023, Microsoft đã phát hành danh sách bản vá tháng 9 với 59 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-2023-36761** trong Microsoft Word cho phép đối tượng tấn công thu thập thông tin về mã băm NTLM của người dùng. Lỗ hổng này hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2023-29332** trong dịch vụ Microsoft Azure Kubernetes Service cho phép đối tượng tấn công không cần xác thực thực hiện tấn công leo thang đặc quyền.

- Lỗ hổng an toàn thông tin **CVE-2023-38148** trong Internet Connection Sharing (ICS) cho phép đối tượng tấn công không cần xác thực thực thi mã từ xa khi ICS được kích hoạt.

- Lỗ hổng an toàn thông tin **CVE-2023-36802** trong Streaming Service Proxy cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. Lỗ hổng này hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2023-38146** trong Windows Themes cho phép đối tượng tấn công thực thi mã từ xa.

- 04 lỗ hổng an toàn thông tin **CVE-2023-36792, CVE-2023-36793, CVE-2023-36794, CVE-2023-36796** trong Visual Studio cho phép đối tượng tấn công thực thi mã từ xa.

- 03 lỗ hổng an toàn thông tin **CVE-2023-36744, CVE-2023-36745, CVE-2023-36756** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.

Thực hiện khuyến nghị của Cục An toàn thông tin (Bộ Thông tin và Truyền thông) tại Công văn số 1664/CATTT-NCSC ngày 21/9/2023 về việc lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 9/2023; Sở Thông tin và Truyền thông tỉnh Gia Lai 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 9/2023, 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.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

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

Đặng Quang Khanh

Phụ lục:

THÔNG TIN VỀ LỖ HỔNG BẢO MẬT ẢNH HƯỞNG MỨC CAO VÀ NGHIÊM TRỌNG TRONG CÁC SẢN PHẨM MICROSOFT CÔNG BỐ THÁNG 9/2023 VÀ HƯỚNG DẪN XỬ LÝ, KHẮC PHỤC LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số: 1648/STTTT-CNTT ngày 26 tháng 9 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-2023-36761	- Điểm: CVSS: 6.2 (Cao) - Mô tả: Lỗ hổng trong Microsoft Word cho phép đối tượng tấn công thu thập thông tin về mã băm NTLM của người dùng. Lỗ hổng này hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft Word, Microsoft 365.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36761
2	CVE-2023-29332	- Điểm: CVSS: 7.5 (Nghiêm trọng) - Mô tả: Lỗ hổng trong dịch vụ Microsoft Azure Kubernetes Service cho phép đối tượng tấn công không cần xác thực thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Microsoft Azure Kubernetes Service.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29332
3	CVE-2023-38148	- Điểm: CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Internet Connection Sharing (ICS) cho phép đối tượng tấn công không cần xác thực thực thi mã từ xa khi ICS được kích hoạt. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38148
4	CVE-2023-36802	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Streaming Service Proxy cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng này hiện đang bị	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36802

		khai thác trong thực tế. - Ảnh hưởng: Windows 11.	
5	CVE-2023-38146	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Windows Themes cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38146
6	CVE-2023-36792 CVE-2023-36793 CVE-2023-36794 CVE-2023-36796	- Điểm: CVSS: 7.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Visual Studio cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft .NET Framework.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36792 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36793 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36794 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36796
7	CVE-2023-36744 CVE-2023-36745 CVE-2023-36756	- 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.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36744 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36745 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36756

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/2023/9/12/the-september-2023-security-update-review