

Số: 406/STTTT-CNTT

Gia Lai, ngày 20 tháng 3 năm 2023

V/v cảnh báo lỗ hổng bảo mật
ảnh hưởng cao và nghiêm trọng
trong các sản phẩm Microsoft
công bố tháng 3/2023

Kính gửi:

- Công an tỉnh;
- 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;
- 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.

Ngày 14/3/2023, Microsoft đã phát hành danh sách bản vá tháng 3 với 74 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 bảo mật **CVE-2023-23397** trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế.

- Lỗ hổng bảo mật **CVE-2023-24880** trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đang bị khai thác trong thực tế.

- Lỗ hổng bảo mật **CVE-2023-23392** trong HTTP Protocol Stack cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-23415** trong Internet Control Message Protocol (ICMP) cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-23399** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-23400** trong Windows DNS 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 383/CATTT-NCSC ngày 17/3/2023 về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 3/2023; 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 3/2023, 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 trong 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 tỉnh Gia Lai 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;
- Văn phòng Tỉnh ủy;
- Lưu: VT, P. CNTT.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

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 3/2023 VÀ HƯỚNG DẪN XỬ LÝ,
KHẮC PHỤC LỖ HỔNG BẢO MẬT**

*(Kèm theo Công văn số: 406/STTTT-CNTT ngày 20 tháng 3 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-2023-23397	<ul style="list-style-type: none"> - Điểm: CVSS: 9.1 (nghiêm trọng) - Mô tả: lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft Outlook, Microsoft Office. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397
2	CVE-2023-24880	<ul style="list-style-type: none"> - Điểm: CVSS: 5.4 (trung bình) - Mô tả: lỗ hổng trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Windows Server, Windows 10/11. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24880
3	CVE-2023-23392	<ul style="list-style-type: none"> - Điểm: CVSS: 9.8 (nghiêm trọng) - Mô tả: lỗ hổng trong HTTP Protocol Stack cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server, Windows 11. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23392
4	CVE-2023-23415	<ul style="list-style-type: none"> - Điểm: CVSS: 9.8 (nghiêm trọng) - Mô tả: lỗ hổng trong Internet Control Message Protocol (ICMP) cho phép đối tượng tấn công thực thi 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23415

Số TT	CVE	Mô tả	Link tham khảo
		mã từ xa. - Ảnh hưởng: Windows Server, Windows 10/11.	
5	CVE-2023-23399	- Điểm: CVSS: 7.8 (cao) - Mô tả: lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office, Microsoft Excel, Microsoft 365 .	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23399
6	CVE-2023-23400	- Điểm: CVSS: 7.2 (cao) - Mô tả: lỗ hổng trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23400

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.

3. Tài liệu tham khảo:

- <https://msrc.microsoft.com/update-guide>
- <https://www.zerodayinitiative.com/blog/2023/3/14/the-march-2023-security-update-review>