

ỦY BAN NHÂN DÂN
XÃ IA O

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

Số: /CV-UBND

la O, ngày tháng năm

V/v cảnh báo lỗ hổng bảo mật
ảnh hưởng cao và nghiêm trọng
trong các sản phẩm Microsoft công bố
tháng 01/2023

Kính gửi:

- Các ban ngành, đoàn thể xã;

Ngày 10/01/2023, Microsoft đã phát hành danh sách bản vá tháng 01 với 98 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-2023-21674** trong Windows Advanced Local Procedure Call (ALPC) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. **Lỗ hổng này đang bị khai thác trong thực tế.**

- 03 lỗ hổng bảo mật **CVE-2023-21743, CVE-2023-21744, CVE-2023-21742** trong Microsoft SharePoint Server, trong đó **CVE-2023-21743** cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật; 02 lỗ hổng **CVE-2023-21744, CVE-2023-21742** cho phép đối tượng tấn công thực thi mã từ xa.

- 04 lỗ hổng bảo mật **CVE-2023-21763, CVE-2023-21764, CVE-2023-21762, CVE-2023-21745** trong Microsoft Exchange Server, trong đó 02 lỗ hổng **CVE-2023-21763, CVE-2023-21764** cho phép đối tượng tấn công thực hiện nâng cao đặc quyền; 02 lỗ hổng **CVE-2023-21762, CVE-2023-21745** cho phép đối tượng tấn công thực hiện tấn công giả mạo.

- Lỗ hổng bảo mật **CVE-2023-21549** trong Windows Workstation Service cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã được công bố rộng rãi trên Internet.

- 02 lỗ hổng bảo mật **CVE-2023-21561, CVE-2023-21551** trong Microsoft Cryptographic Services cho phép đối tượng tấn công nâng cao đặc quyền.

- 02 lỗ hổng bảo mật **CVE-2023-21734, CVE-2023-21735** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.

Thực hiện khuyến nghị của Sở Thông tin và Truyền thông tỉnh Gia Lai tại Công văn số 65/STTTT-CNTT ngày 13/01/2023 về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2023; và công văn số 06/PVHTT ngày 02/02/2023 của Phòng Văn hóa và Thông tin huyện về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2023. UBND xã đề nghị các ban ngành, đoàn thể xã 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 01/2023, 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.

UBND xã đề nghị các ban ngành, đoàn thể phối hợp, triển khai thực hiện./.

Nơi nhận:

- Như trên;
- Lưu: VT.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Kpã Geo

Phu lục:

**THÔNG TIN VỀ LỖ HỒNG BẢO MẬT ẢNH HƯỞNG MỨC CAO
VÀ NGHIÊM TRỌNG TRONG CÁC SẢN PHẨM MICROSOFT
CÔNG BỐ THÁNG 01/2023 VÀ HƯỚNG DẪN XỬ LÝ,
KHẮC PHỤC LỖ HỒNG BẢO MẬT**

*(Kèm theo Công văn số: /CV-UBND ngày tháng 02 năm 2023
của UBND xã Ia O)*

1. Thông tin các lỗ hồng bảo mật:

Số TT	CVE	Mô tả	Link tham khảo
1	CVE-2023-21674	<ul style="list-style-type: none"> - Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hồng trong Windows Advanced Local Procedure Call (ALPC) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hồng này đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2019/2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21674
2	CVE-2023-21743, CVE-2023-21744, CVE-2023-21742	<ul style="list-style-type: none"> - Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hồng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass), thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2019/2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21743 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21744 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21742
3	CVE-2023-21763, CVE-2023-21764, CVE-2023-21762, CVE-2023-21745	<ul style="list-style-type: none"> - Điểm: CVSS: 8.0/7.8 (cao) - Mô tả: lỗ hồng trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền, tấn công giả mạo (Spoofing). - Ảnh hưởng: Microsoft Exchange Server 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21763 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21764 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21762 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21745

		2016/2019.	guide/vulnerability/CVE-2023-21762 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21745
4	CVE-2023-21549	- Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hổng trong Windows Workstation Service cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã được công bố rộng rãi trên Internet. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2012/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21549
5	CVE-2023-21561, CVE-2023-21551	- Điểm: CVSS: 8.8/7.8 (cao) - Mô tả: lỗ hổng trong Microsoft Cryptographic Services cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21561 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21551
6	CVE-2023-21734, CVE-2023-21735	- Điểm: CVSS: 7.8 (cao) - Mô tả: lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office LTSC for Mac 2021, Microsoft 365, Microsoft Office 2019 for Mac.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21734 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21735

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/2023/1/10/the-january-2023-security-update-review>