

**ỦY BAN NHÂN DÂN
HUYỆN IA GRAI**

Số: /UBND-VHTT

V/v cảnh báo lỗ hổng bảo mật
ảnh hưởng cao trong các sản phẩm
Microsoft công bố tháng 5/2023

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

Ia Grai, ngày tháng 5 năm 2023

Kính gửi:

- Các cơ quan, đơn vị thuộc huyện;
- Ủy ban nhân dân các xã, thị trấn.

Ủy ban nhân dân huyện nhận được Công văn số 836/STTTT-CNTT ngày 18/5/2023 của Sở Thông tin và Truyền thông tỉnh Gia Lai về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 5/2023. Ngày 09/5/2023, Microsoft đã phát hành danh sách bản vá tháng 5 với 38 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-2023-24955** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

Trong tháng 01 vừa qua, đã có hai lỗ hổng bảo mật được công bố với mã là CVE-2023-21744, CVE-2023-21742 liên quan đến Microsoft SharePoint Server, những lỗ hổng này cho phép đối tượng tấn công thực thi mã từ xa, đã được Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) cảnh báo trong Văn bản số 50/CATTT-NCSC ngày 11/01/2023 về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2023 (nội dung này UBND huyện đã triển khai tại Công văn số 106/UBND-VHTT ngày 03/02/2023 theo hướng dẫn của Sở TT&TT gửi cho các đơn vị để tự kiểm tra, rà soát). Qua đó cho thấy, Microsoft SharePoint Server đã và đang là mục tiêu nhắm đến của nhiều đối tượng tấn công mạng nhằm thực hiện các hành động trái phép. Chính vì vậy, các cơ quan, tổ chức cần đặc biệt quan tâm và có phương án khắc phục, xử lý kịp thời nếu bị ảnh hưởng.

- 02 lỗ hổng bảo mật **CVE-2023-29336, CVE-2023-24902** trong Win32k 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-2023-29325** trong Windows OLE cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đã được công bố rộng rãi trên Internet.

- Lỗ hổng bảo mật **CVE-2023-24941** trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-24932** trong Secure Boot cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đã được công bố rộng rãi trên Internet.

- Lỗ hổng bảo mật **CVE-2023-29344** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-24953** trong Microsoft Excel 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 729/CATTT-NCSC ngày 15/5/2023 về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 5/2023, Ủy ban nhân dân huyện yêu cầu 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 5/2023, 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.

Ủy ban nhân dân huyện yêu cầu các cơ quan, đơn vị triển khai thực hiện./.

Nơi nhận:

- Như trên;
- Lãnh đạo UBND huyện;
- CVP, PCVP, CV(theo dõi);
- Phòng VH TT;
- Lưu: VT, VH TT.

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

Đỗ Văn Đông

Phụ lục:

**THÔNG TIN VỀ LỖ HỒNG BẢO MẬT ẢNH HƯỞNG MỨC CAO
VÀ NGHIÊM TRỌNG TRONG CÁC SẢN PHẨM MICROSOFT
CÔNG BỐ THÁNG 5/2023 VÀ HƯỚNG DẪN XỬ LÝ,
KHẮC PHỤC LỖ HỒNG BẢO MẬT**

*(Kèm theo Công văn số: 836/STTTT-CNTT ngày 18 tháng 5 năm 2023
của Sở Thông tin và Truyền thông tỉnh Gia Lai)*

1. Thông tin các lỗ hồng bảo mật:

Số TT	CVE	Mô tả	Link tham khảo
1	CVE-2023-24955	- Điểm: CVSS: 7.2 (cao) - Mô tả: lỗ hồng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24955
2	CVE-2023-29336 CVE-2023-24902	- Điểm: CVSS: 7.8 (cao) - Mô tả: lỗ hồng trong Win32k cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hồng này đang bị khai thác trong thực tế. - Ảnh hưởng: Windows Server, Windows 10,11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29336 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24902
3	CVE-2023-29325	- Điểm: CVSS: 8.1 (cao) - Mô tả: lỗ hồng trong Windows OLE cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hồng này đã được công bố rộng rãi trên Internet. - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29325
4	CVE-2023-24941	- Điểm: CVSS: 9.8 (nghiêm trọng) - Mô tả: lỗ hồng trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24941

5	CVE-2023-24932	- Điểm: CVSS: 6.7 (trung bình) - Mô tả: lỗ hổng trong Secure Boot cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đã được công bố rộng rãi trên Internet. - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24932
6	CVE-2023-29344	- 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, Microsoft 365.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29344
7	CVE-2023-24953	- 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 365, Microsoft Excel.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24953

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/2023/5/8/the-may-2023-security-update-review>