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: 415/STTTT-CNTT
V/v cảnh báo lỗ hổng bảo mật có mức ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 3/2022

*Gia Lai, ngày 22 tháng 3 năm 2022*

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 08/3/2022, Microsoft đã phát hành danh sách bản vá tháng 3 với 71 lỗ hổng bảo mật trong các sản phẩm của mình. Bản phát hành tháng 3 này đặc biệt đáng chú ý các lỗ hổng bảo mật có mức ảnh hưởng Cao, cụ thể như sau:

- 02 lỗ hổng bảo mật CVE-2022-21990, CVE-2022-23285 trong Remote Desktop Client cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đã có mã khai thác được công bố rộng rãi trên Internet.

- Lỗ hổng bảo mật CVE-2022-24459 trong Windows Fax và Scan Service cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền.

- Lỗ hổng bảo mật CVE-2022-24508 trong SMBv3 cho phép đối tượng tấn công thực thi mã từ xa trên Windows SMBv3 Client/Server.

- Lỗ hổng bảo mật CVE-2022-23277 trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa với tài khoản xác thực hợp lệ.

- Lỗ hổng bảo mật CVE-2022-21967 trong Xbox Live Auth Manager for Windows cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền.

- Lỗ hổng bảo mật CVE-2022-22006 trong HEVC Video Extensions cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2022-24501 trong cho phép đối tượng tấn công thực thi mã từ xa.

Thực hiện khuyến nghị của Cục An toàn thông tin tại Công văn số 315/CATTT-NCSC ngày 09/3/2022 về việc lỗ hổng bảo mật có mức ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 3/2022; 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 cao trong các sản phẩm Microsoft công bố tháng 3/2022, cụ thể như sau:

**1.** Kiểm tra, rà soát, xác định máy chủ sử dụng đệ điều hành Windows có khả năng bị ảnh hưởng bởi lỗ hổng bảo mật trên để có phương án xử lý, khắc phục lỗ hổng. 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**

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 CAO TRONG CÁC SẢN PHẨM MICROSOFT CÔNG BỐ THÁNG 3/2022 VÀ HƯỚNG DẪN XỬ LÝ, KHẮC PHỤC LỖ HỔNG BẢO MẬT**

*(Kèm theo Công văn số: 415/STTTT-CNTT ngày 22 tháng 3 năm 2022 của Sở Thông tin và Truyền thông tỉnh Gia Lai)*

**1. Thông tin các lỗ hổng bảo mật:**

| Số TT | Tên lỗ hổng | Mô tả | Link tham khảo |
|---|---|---|---|
| 1 | CVE-2022-21990 | - Điểm CVSS: 8.8 (Cao)<br>- Lỗ hổng trong Remote Desktop Client cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 11/10/8.1/7. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21990 |
| 2 | CVE-2022-23285 | - Điểm CVSS: 8.8 (Cao)<br>- Lỗ hổng trong Remote Desktop Client cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 10/8.1/7. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23285 |
| 3 | CVE-2022-24459 | - Điểm CVSS: 7.8 (Cao)<br>- Lỗ hổng Windows Fax và Scan Service cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền.<br>- Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 11/10/8.1/7. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24459 |

| | | | |
|---|---|---|---|
| 4 | CVE-2022-24508 | - Điểm CVSS: 8.8 (Cao)<br>- Lỗ hổng trong trong SMBv3 cho phép đối tượng tấn công thực thi mã từ xa trên Windows SMBv3 Client/Server.<br>- Ảnh hưởng: Windows 10/11, Windows Server 2022. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24508 |
| 5 | CVE-2022-23277 | - Điểm CVSS: 8.8 (Cao)<br>- Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa với tài khoản xác thực hợp lệ.<br>- Ảnh hưởng: Microsoft Exchange Server 2019/2016/2013. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23277 |
| 6 | CVE-2022-21967 | - Điểm CVSS: 7.0 (Cao)<br>- Lỗ hổng trong trong Xbox Live Auth Manager for Windows cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền.<br>- Ảnh hưởng: Windows 10/11. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21967 |
| 7 | CVE-2022-22006 | - Điểm CVSS: 7.8 (Cao)<br>- Lỗ hổng trong HEVC Video Extensions, cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: HEVC Video Extensions. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22006 |
| 8 | CVE-2022-24501 | - Điểm CVSS: 7.8 (Cao)<br>- Lỗ hổng trong VP9 Video Extensions, cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: VP9 Video Extensions. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24501 |

**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/releaseNote/2022-Mar*

- *https://msrc.microsoft.com/update-guide/en-us*