UBND TỈNH GIA LAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 2366/STTTT-CNTT

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 12/2021

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

Gia Lai, ngày 22 tháng 12 năm 2021

Kính gửi:

- Công an tỉnh;
- Bộ Chỉ huy Quân sự tỉnh;
- Bộ Chỉ huy Bộ đội biên phòng tỉnh;
- Văn phòng Tỉnh ủy;
- 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 14/12/2021, Microsoft đã phát hành danh sách bản vá tháng 12 với 67 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 sau:

1. Các lỗ hổng có mức ảnh hưởng Nghiêm trọng:

- Lỗ hổng bảo mật CVE-2021-43907 trong Windows Sybsystem for Linux (WSL), cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2021-43899 trong Microsoft 4K Wireless Display Adapter, cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2021-43215 trong iSNS Server, cho phép đối tượng tấn công thực thi mã từ xa.

2. Các lỗ hổng có mức ảnh hưởng Cao:

- Lỗ hổng bảo mật CVE-2021-43890 trong Windows AppX Installer, cho phép đối tượng tấn công thực hiện tấn công giả mạo. Bên cạnh đó, lỗ hổng này được cho là đang được khai thác trong chiến dịch tấn công mã độc Emotet, Trickbot, Bazaloader.

- Lỗ hổng bảo mật CVE-2021-42309 trong Microsoft SharePoint Server, cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2021-41333 trong Windows Print Spooler, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật CVE-2021-43880 trong Windows Mobile Device Management, cho phép đối tượng tấn công nâng cao đặc quyền, xóa tệp tin trong hệ thống mục tiêu.

- Lỗ hổng bảo mật CVE-2021-43893 trong Windows Encrypting File System (EFS), cho phép đối tượng tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật CVE-2021-43240 trong NTFS Set Short Name, cho phép đối tượng tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật CVE-2021-43883 trong Windows Installer cho phép đối tượng tấn công leo thang đặc quyền.

Thực hiện khuyến nghị của Cục An toàn thông tin tại Công văn số 1749/CATTT-NCSC ngày 15/12/2021 về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 12/2021; 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 và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 12/2021, 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 cho các lỗ hổng bảo mật (*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;
- 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 VÀ NGHIÊM TRỌNG TRONG CÁC SẢN PHẨM MICROSOFT CÔNG BỐ THÁNG 12/2021 VÀ HƯỚNG DẪN XỬ LÝ, KHẮC PHỤC LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số: 2366/STTTT-CNTT ngày 22 tháng 12 năm 2021 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-2021-43890	- Điểm CVSS: 7.1 (cao) - Lỗ hổng trong Windows AppX Installer, cho phép đối tượng tấn công thực hiện tấn công giả mạo.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-43890
2	CVE-2021-43907	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows Subsystem for Linux (WSL), cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Visual Studio Code WLS Extension	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43907
3	CVE-2021-42309	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Microsoft SharePoint Server, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Foundation 2013, SharePoint Server 2019, SharePoint Enterprise Server 2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-42309
4	CVE-2021-43899	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Microsoft 4K Wireless Display Adapter, cho	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-43899

		phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft 4K Wireless Display Adapter	
5	CVE-2021-43215	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong iSNS Server, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008/2012/2016/2019, Windows 7/8.1/10.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43215
6	CVE-2021-41333	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Print Spooler, cho phép đối tượng tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2019/2016/2012/2008, Windows 8.1/7/10.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-41333
7	CVE-2021-43880	- Lỗ hổng trong Windows Mobile Device Management, cho phép đối tượng tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows 11	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43880
8	CVE-2021-43893	- Điểm CVSS: 7.5 (cao) - Lỗ hổng trong Windows Encrypting File System (EFS) cho phép đối tượng tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows 10/11, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43893

9	CVE-2021-43240	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong NTFS Set Short Name cho phép đối tượng tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows 10/11, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43240
10	CVE-2021-43883	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Installer, cho phép đối tượng tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2022/2019/2016/2012/2008, Windows 11/10/8.1/7	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43883

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/en-us*