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: 186/STTTT-CNTT

Gia Lai, ngày 11 tháng 02 năm 2022

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 02/2022

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 08/02/2022, Microsoft đã phát hành danh sách bản vá tháng 02 với 48 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 sau:

- Lỗ hổng bảo mật CVE-2022-22005 trong Sharepoint Server 2013-2019 cho phép đối tượng tấn công thực thi mã từ xa với tài khoản xác thực hợp lệ.

- Lỗ hổng bảo mật CVE-2022-21989 trong Windows Kernel cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật CVE-2022-21984 trong DNS Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2022-21995 trong Windows Hyper-V cho phép đối tượng tấn công đã xác thực trên máy khách Hyper-V có thể thực thi mã từ xa trên máy chủ Hyper-V.

- 02 lỗ hổng bảo mật CVE-2022-22718, CVE-2022-21999 trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- 02 lỗ hổng bảo mật CVE-2022-22000, CVE-2022-21981 trong Windows Common Log File System Driver cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật CVE-2022-21996 trong Windows32k cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật CVE-2022-22715 trong Named Pipe File System cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

Thực hiện khuyến nghị của Cục An toàn thông tin tại Công văn số 163/CATTT-NCSC ngày 09/02/2022 về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 02/2022; 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 và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 02/2022, 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;
- 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 02/2022 VÀ HƯỚNG DẪN XỬ LÝ, KHẮC PHỤC LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số: 186/STTTT-CNTT ngày 11 tháng 02 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-2022-22005	- 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 Server 2019, SharePoint Enterprise Server 2013/2016.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-22005
2	CVE-2022-21989	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Microsoft Kernel, cho phép đối tượng tấn công thực hiện 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/en-US/vulnerability/CVE-2022-21989
3	CVE-2022-21984	- Điểm CVSS: 8.8 (cao) - Lỗ hổng trong Windows DNS Server, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10/11, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21984

4	CVE-2022-21995	- Điểm CVSS: 7.9 (cao) - Lỗ hổng trong Windows Hyper-V, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10/11, Windows Server 2022/2019/2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21995
5	CVE-2022-22718	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Print Sooler, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2022/2016/2012/2008, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22718
6	CVE-2022-22000	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Common Log File System Driver, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows Server 2022/2019/2016/2012/2008, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22000
7	CVE-2022-21999	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Print Sooler, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows Server	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21999

		2022/2016/2012/2008, Windows 11/10/8.1/7.	
8	CVE-2022-21981	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Common Log File System Driver, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows Server 2019/2012/2008, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21981
9	CVE-2022-21996	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows32k, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows 11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21996
10	CVE-2022-22715	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Named Pipe File System, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows 11/10, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22715

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/2022/2/8/the-february-2022-security-update-review*