UBND TỈNH GIA LAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 74/STTTT-CNTT

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2022

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

Gia Lai, ngày 14 tháng 01 năm 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 11/01/2022, Microsoft đã phát hành danh sách bản vá tháng 1 với 96 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-2022-21907 trong HTTP Protocol Stack (http.sys) của Windows, cho phép đối tượng tấn công thực thi mã từ xa mà không cần xác thực.

2. Các lỗ hổng có mức ảnh hưởng cao:

- 03 lỗ hổng bảo mật CVE-2022-21846, CVE-2022-21969, CVE-2022-21855 trong Microsoft Exchange Server, cho phép đối tượng tấn công thực thi mã từ xa. Để khai thác lỗ hổng này, kẻ tấn công cần có quyền truy cập vào mạng mục tiêu từ đấy có thể chiếm quyền điều khiển máy chủ.

- Lỗ hổng bảo mật CVE-2022-21857 trong Active Directory, cho phép đối tượng nâng cao đặc quyền.

- Lỗ hổng bảo mật CVE-2022-21840 trong Microsoft Office, cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2022-21911 trong .NET Framework, cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ.

- Lỗ hổng bảo mật CVE-2022-21836 trong Windows Certificate, cho phép đối tượng tấn công giả mạo.

- Lỗ hổng bảo mật CVE-2022-21841 trong Microsoft Excel, cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2022-21837 trong Microsoft SharePoint Server, cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2022-21842 trong Microsoft Word, 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 56/CATTT-NCSC ngày 12/01/2022 về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2022; 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 01/2022, 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 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 01/2022 VÀ HƯỚNG DẪN XỬ LÝ, KHẮC PHỤC LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số: 74/STTTT-CNTT ngày 14 tháng 01 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-2022-21907	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong HTTP Protocol, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server 2019/2022, Windows 11/10.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21907
2	CVE-2022-21846	- Điểm CVSS: 9.0 (Cao) - Lỗ hổng trong Exchange Server, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Exchange Server 2019/2016/2013.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21846
3	CVE-2022-21855	- Điểm CVSS: 9.0 (Cao) - Lỗ hổng trong Exchange Server, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Exchange Server 2019/2016/2013.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21855
4	CVE-2022-21969	- Điểm CVSS: 9.0 (Cao) - Lỗ hổng trong Exchange Server, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Exchange Server	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21969

		2019/2016/2013.	
5	CVE-2022-21840	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Microsoft Office, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Foundation 2013, SharePoint Server 2019, Microsoft Office 2016/2013/LTSC 2021/2019, Microsoft Excel 2016/2013, Microsoft 365	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21840
6	CVE-2022-21875	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Active Directory Domain Services, cho phép đối tượng tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2022/2019/2016/2012/2008, Windows 11/10/RT 8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21857
7	CVE-2022-21911	- Điểm CVSS: 7.5 (Cao) - Lỗ hổng trong .NET Framework, cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ. - Ảnh hưởng: Microsoft .NET Framework 3.5 AND 4.7.2, 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2,…	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21911
8	CVE-2022-21836	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Certificate, cho phép đối tượng tấn công thực hiện tấn công giả	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21836

		mạo - Ảnh hưởng: Windows Server 2022/2019/2016/2012/2008, Windows 10/RT 8.1/7.	
9	CVE-2022-21841	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Microsoft Excel, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office 2013/2016/2019/LTSC2021, Microsoft 365.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21841
10	CVE-2022-21837	- Điểm CVSS: 8.3 (cao) - Lỗ hổng trong Microsoft SharePoint Server, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server 2019, 2016	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21837
11	CVE-2022-21842	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Microsoft Word, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Word 2016.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21842

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-Jan*

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