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: 1968/STTTT-CNTT

Gia Lai, ngày 15 tháng 12 năm 2022

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 12/2022

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 13/12/2022, Microsoft đã phát hành danh sách bản vá tháng 12 với 52 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, cụ thể như sau:

- Lỗ hổng bảo mật **CVE-2022-44698** trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật. Lỗ hổng này đang bị khai thác trong thực tế.

- Lỗ hổng bảo mật **CVE-2022-41076** trong PowerShell cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này ảnh hưởng đến nhiều sản phẩm như: Microsoft Exchange Server, Skype for Business Server,…

- Lỗ hổng bảo mật **CVE-2022-44713** trong Microsoft Outlook for Mac cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing).

- Lỗ hổng bảo mật **CVE-2022-44699** trong Azure Network Watcher Agent cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật.

- Lỗ hổng **CVE-2022-44710** trong DirectX Graphics Kernel cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã có mã khai thác được công bố rộng rãi trên Internet.

- 02 lỗ hổng bảo mật **CVE-2022-44690, CVE-2022-44693** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- 02 lỗ hổng bảo mật **CVE-2022-44678, CVE-2022-44681** trong Windows Print Spooler cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

- 02 lỗ hổng bảo mật **CVE-2022-44708, CVE-2022-41115** trong Microsoft Edge (Chromium-based) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-44673** trong Windows Client Server Run-Time Subsystem (CSRSS) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

Thực hiện khuyến nghị của Cục An toàn thông tin tại Công văn số 2035/CATTT-NCSC ngày 14/12/2022 về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 12/2022; 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 mức cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 12/2022, 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.

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 MỨC CAO VÀ NGHIÊM TRỌNG TRONG CÁC SẢN PHẨM MICROSOFT CÔNG BỐ THÁNG 12/2022 VÀ HƯỚNG DẪN XỬ LÝ, KHẮC PHỤC LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số: 1968/STTTT-CNTT ngày 15 tháng 12 năm 2022 của Sở Thông tin và Truyền thông tỉnh Gia Lai)

1. Thông tin các lỗ hổng bảo mật:

Số TT	CVE	Mô tả	Link tham khảo
1	CVE-2022-44698	- Điểm: CVSS: 5.4 - Mô tả: lỗ hổng trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật. Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10/11, Windows Server 2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44698
2	CVE-2022-41076	- Điểm CVSS: 8.5 (Cao) - Mô tả: lỗ hổng trong PowerShell cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022, PowerShell 7.2/7.3.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41076
3	CVE-2022-44713	- Điểm CVSS: 7.5 (Cao) - Mô tả: lỗ hổng trong Microsoft Outlook for Mac cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). - Ảnh hưởng: Microsoft Office 2019 for Mac, Office LTSC for Mac 2021.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44713
4	CVE-2022-44699	- Điểm CVSS: 5.5 - Mô tả: lỗ hổng trong Azure Network Watcher Agent cho phép đối tượng	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44699

Số TT	CVE	Mô tả	Link tham khảo
		tấn công thực hiện tấn công vượt qua cơ chế bảo mật. - Ảnh hưởng: Azure Network Watcher Vm Extension.	
5	CVE-2022-44710	- Điểm CVSS: 7.8 (Cao) - Mô tả: lỗ hổng trong DirectX Graphics Kernel cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã có mã khai thác được công bố rộng rãi trên Internet. - Ảnh hưởng: Windows 11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44710
6	CVE-2022-44678, CVE-2022-44681	- Điểm CVSS: 8.8 (Cao) - Mô tả: lỗ hổng trong Windows Print Spooler cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44678 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44681
7	CVE-2022-44690, CVE-2022-44693	- Điểm CVSS: 8.8 (Cao) - Mô tả: trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server 2019, SharePoint Foundation 2013, SharePoint Enterprise Server 2013/2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44690 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44693
8	CVE-2022-44708, CVE-2022-41115	- Điểm CVSS: 8.3 (Cao) - Mô tả: Lỗ hổng trong Microsoft Edge (Chromium-based) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Microsoft Edge	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44708 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41115

Số TT	CVE	Mô tả	Link tham khảo
9	CVE-2022-44673	- Điểm CVSS: 7.0 (Cao) - Mô tả: Lỗ hổng trong Windows Client Server Run-Time Subsystem (CSRSS) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows 7/8.1/10, Windows Server 2008.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44673

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
- https://www.zerodayinitiative.com/blog/2022/12/13/the-december-2022-security-update-review