

**BỘ THÔNG TIN TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN**

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

Số: /CATTT-NCSC
V/v lỗ hổng bảo mật ảnh hưởng mức Cao
và Nghiêm trọng trong các sản phẩm
Microsoft công bố tháng 9/2022

Hà Nội, ngày tháng năm 2022

Kính gửi:

- Đơn vị chuyên trách về CNTT các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước; các Ngân hàng TMCP; các tổ chức tài chính;
- Hệ thống các đơn vị chuyên trách về an toàn thông tin.

Ngày 13/9/2022, Microsoft đã phát hành danh sách bản vá tháng 9 với 64 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 sau:

- Lỗ hổng bảo mật **CVE-2022-37969** trong Windows Common Log File System Driver cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đang được khai thác rộng rãi trên Internet.

- Lỗ hổng bảo mật **CVE-2022-34718** trong Windows TCP/IP cho phép đối tượng tấn công chưa xác thực có thể thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-34724** trong Windows DNS Server cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ.

- Lỗ hổng bảo mật **CVE-2022-3075** trong Chromium cho phép đối tượng tấn công chưa xác thực có thể thực thi mã từ xa.

- 02 lỗ hổng bảo mật **CVE-2022-34721, CVE-2022-34722** trong Windows Internet Key Exchange (IKE) Protocol Extensions cho phép đối tượng tấn công thực thi mã từ xa. Mã khai thác của các lỗ hổng này đã được công bố rộng rãi trên Internet.

- 04 lỗ hổng bảo mật **CVE-2022-37961, CVE-2022-35823, CVE-2022-38008, CVE-2022-38009** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-37962** trong Microsoft PowerPoint cho phép

đối tượng tấn công thực thi mã từ xa khi người dùng mở tập tin PowerPoint độc hại.

Thông tin chi tiết các lỗ hổng bảo mật có tại phụ lục kèm theo.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Cục An toàn thông tin khuyến nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát, xác định máy sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công (tham khảo thông tin tại phụ lục kèm theo).

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.

3. Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ais@mic.gov.vn.

Trân trọng./.

Nơi nhận:

- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Huy Dũng (để b/c);
- Cục A05, Bộ Công an;
- Bộ Tư lệnh 86, Bộ Quốc phòng;
- Ban Cơ yếu Chính phủ;
- Cục trưởng (để b/c);
- PCT Trần Đăng Khoa;
- Trung tâm VNCERT/CC, phòng ATHTTT;
- Lưu: VT, NCSC.

**KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG**

Trần Đăng Khoa

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT
TRONG SẢN PHẨM MICROSOFT

(Kèm theo Công văn số /CATT-NCSC ngày / /2022
của Cục An toàn thông tin)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-37969	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows Common Log File System Driver cho phép đối tượng tấn công thực thi mã từ xa với các đặc quyền nâng cao. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37969
2	CVE-2022-34718	<ul style="list-style-type: none"> - Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows TCP/IP cho phép đối tượng tấn công chưa xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34718
3	CVE-2022-34724	<ul style="list-style-type: none"> - Điểm CVSS: 7.5 (Cao) - Lỗ hổng trong Windows DNS Server cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34724
4	CVE-2022-3075	<ul style="list-style-type: none"> - Lỗ hổng trong Chromium cho phép đối tượng tấn công chưa xác 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3075

		<p>thực có thể thực thi mã từ xa.</p> <ul style="list-style-type: none"> - Ảnh hưởng: Microsoft Edge (Chromium-based) 	
5	CVE-2022-34721, CVE-2022-34722	<ul style="list-style-type: none"> - Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows Internet Key Exchange (IKE) Protocol Extensions 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. 	<p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34721</p> <p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34722</p>
6	CVE-2022-37961 CVE-2022-35823 CVE-2022-38008 CVE-2022-38009	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SherePoint Foundation 2013, SharePoint Server 2013/2016/2019, Microsoft SharePoint Enterprise Server 2013. 	<p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37961</p> <p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35823</p> <p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38008</p> <p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38009</p>
7	CVE-2022-37962	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft PowerPoint cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office 2013/2016/2019, Office 365 Apps, Office LTSC 2021. 	<p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37962</p>

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng bảo mật nói trên theo hướng dẫn của hãng. Quý đơn vị tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại link nguồn tham khảo tại mục 1 của phụ lục.

3. Tài liệu tham khảo

<https://msrc.microsoft.com/update-guide/releaseNote/2022-Sep>

<https://www.zerodayinitiative.com/blog/2022/9/13/the-september-2022-security-update-review>