

Số: /TTCNTT-KTHT
V/v lỗ hổng bảo mật ảnh hưởng Cao và
Nghiêm trọng trong các sản phẩm
Microsoft công bố tháng 05/2022

Hà Nội, ngày tháng năm 2022

Kính gửi: Các đơn vị trực thuộc Bộ

Ngày 10/5/2022, Microsoft đã phát hành danh sách bản vá tháng 5 với 74 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:

Các lỗ hổng bảo mật có mức ảnh hưởng Nghiêm trọng:

- Lỗ hổng bảo mật **CVE-2022-26925** trong Windows LSA cho phép đối tượng tấn công không cần xác thực có thể thực hiện tấn công giả mạo (spoofing). Trong thực tế, lỗ hổng này đang được sử dụng kết hợp với NTLM relay attack, từ đó giúp đối tượng tấn công nâng cao đặc quyền trong hệ thống mục tiêu.

- Lỗ hổng bảo mật **CVE-2022-26937** trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-29972** trong Magnitude Simba Amazon Redshift ODBC Driver cho phép đối tượng thực thi mã từ xa.

Các lỗ hổng bảo mật có mức ảnh hưởng Cao:

- Lỗ hổng bảo mật **CVE-2022-26923** trong Active Directory Domain Services cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-21978** trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-22017** trong Remote Desktop Protocol Client cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-29110** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-29108** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

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

Nhằm bảo đảm an toàn thông tin cho hệ thống thông tin của Quý đơn vị, Trung tâm Công nghệ thông tin khuyến nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát, xác định máy tính 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.

Trong trường hợp cần thiết, Quý đơn vị liên hệ đầu mối hỗ trợ của Trung tâm Công nghệ thông tin: Phòng Kỹ thuật hạ tầng, điện thoại 024.39439060, thư điện tử: phongktht@most.gov.vn.

Trân trọng./.

Nơi nhận:

- Như trên;
- Thứ trưởng Bùi Thế Duy (để b/c);
- Cổng thông tin điện tử Bộ KH&CN;
- Lưu: VT, KTHT.

GIÁM ĐỐC

Hà Quốc Trung

Phụ lục
Thông tin về các lỗ hổng bảo mật trong sản phẩm Microsoft
(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2022 của Trung tâm Công nghệ thông tin)

1. Thông tin các lỗ hổng bảo mật

TT	CVE	Mô tả	Link tham khảo
1	CVE-2022-26925	<ul style="list-style-type: none">- Điểm CVSS: 9.8 (Nghiêm trọng)- Lỗ hổng trong Windows LSA cho phép đối tượng tấn công không cần xác thực có thể thực hiện tấn công giả mạo (spoofing) kết hợp với NTLM relay attack từ đó nâng cao đặc quyền trong hệ thống mục tiêu.- Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2022/2019/2016/2012/2008.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-26925
2	CVE-2022-26923	<ul style="list-style-type: none">- Điểm CVSS: 8.8 (Cao)- Lỗ hổng trong Active Directory Domain Services cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.- Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24491
3	CVE-2022-26937	<ul style="list-style-type: none">- Điểm CVSS: 9.8 (Nghiêm trọng)- Lỗ hổng trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa.- Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26937
4	CVE-2022-29972	<ul style="list-style-type: none">- Lỗ hổng trong Magnitude Simba Amazon Redshift ODBC	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29972

		Driver cho phép đổi tượng thực thi mã từ xa.	https://msrc-blog.microsoft.com/2022/05/09/vulnerability-mitigated-in-the-third-party-data-connector-used-in-azure-synapse-pipelines-and-azure-data-factory-cve-2022-29972
5	CVE-2022-21978	- Điểm CVSS: 8.2 (Cao) - Lỗ hổng trong Microsoft Exchange Server cho phép đổi tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2013/2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21978
6	CVE-2022-22017	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Remote Desktop Protocol Client cho phép đổi tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 11, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22017
7	CVE-2022-29110	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft Excel cho phép đổi tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office Web Apps Server 2013, Microsoft Excel 2013/2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29110
8	CVE-2022-29108	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft SharePoint Server cho phép đổi tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server 2016/2019, Microsoft SharePoint Foundation 2013.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29108

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. Nguồn tham khảo

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

<https://www.zerodayinitiative.com/blog/2022/5/10/the-may-2022-security-update-review>

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN

(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2022 của Trung tâm Công nghệ thông tin)

TT	Tên đơn vị
1.	Thanh tra Bộ
2.	Cục Công tác phía Nam
3.	Cục Ứng dụng và phát triển công nghệ
4.	Cục Năng lượng nguyên tử
5.	Cục Thông tin Khoa học và Công nghệ Quốc gia
6.	Cục Phát triển thị trường và doanh nghiệp khoa học và công nghệ
7.	Cục An toàn bức xạ và hạt nhân
8.	Cục Sở hữu trí tuệ
9.	Tổng Cục tiêu chuẩn đo lường chất lượng
10.	Ban quản lý khu công nghệ cao Hoà Lạc
11.	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo
12.	Viện Khoa học và công nghệ Việt Nam - Hàn Quốc (VKIST)
13.	Viện Nghiên cứu sáng chế và Khai thác công nghệ
14.	Viện Năng lượng nguyên tử Việt Nam
15.	Viện Ứng dụng công nghệ
16.	Viện Đánh giá khoa học và Định giá công nghệ
17.	Viện Khoa học sở hữu trí tuệ
18.	Viện Nghiên cứu và Phát triển Vùng
19.	Văn phòng các Chương trình trọng điểm cấp nhà nước
20.	Văn phòng Công nhận chất lượng
21.	Văn phòng Đăng ký hoạt động khoa học và công nghệ
22.	Văn phòng các Chương trình khoa học và công nghệ quốc gia
23.	Báo Khoa học và Phát triển
24.	Tạp chí Khoa học và Công nghệ Việt Nam
25.	Nhà xuất bản Khoa học và Kỹ thuật
26.	Quỹ Phát triển khoa học và công nghệ quốc gia
27.	Quỹ Đổi mới công nghệ quốc gia
28.	Trung tâm Nghiên cứu và Phát triển truyền thông khoa học và công nghệ
29.	Trung tâm Nghiên cứu và Phát triển hội nhập khoa học và công nghệ quốc tế