Báo cáo về các lỗ hổng an toàn thông tin trong các sản phẩm của Microsoft tháng 10/2024

1. Thông tin chung

Thực hiện chức năng quản lý nhà nước và tổ chức thực thi pháp luật về an toàn thông tin mạng, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin trong tháng vừa qua đã ghi nhận thông tin về các lỗ hổng an toàn thông tin của hãng Microsoft. Ngày 08/10/2024, Microsoft đã phát hành danh sách bản vá **tháng 10** với tổng **121 lỗ hổng an toàn thông tin** gồm có **117 lỗ hổng an toàn thông tin** trong các sản phẩm của hãng Microsoft và **04 lỗ hổng an toàn thông tin** trong các sản phẩm thuộc bên thứ ba có ảnh hưởng tới Microsoft, trong đó có 03 lỗ hổng mức Nghiêm trọng và 115 lỗ hổng mức độ Cao.

Các lỗ hổng này có mức độ ảnh hưởng **Cao** và **Nghiêm trọng**, có thể bị đối tượng tấn công khai thác để thực hiện các hành vi trái phép, gây ra nguy cơ mất an toàn thông tin và ảnh hưởng đến các hệ thống thông tin của cơ quan, tổ chức và doanh nghiệp.

Lỗ hổng an toàn thông tin tồn tại trên một số sản phẩm của Microsoft như: Windows; Microsoft Office; Azure; .NET và Visual Studio; OpenSSH cho Windows; Power BI; Windows Hyper-V; Windows Mobile Broadband;…

*Thông tin chi tiết về lỗ hổng an toàn thông tin xem tại **mục 2** của báo cáo.*

Đề nghị các cơ quan, đơn vị, doanh nghiệp nghiên cứu thông tin về các lỗ hổng an toàn thông tin dưới đây, thực hiện rà soát hệ thống, xử lý các vấn đề về an toàn thông tin mạng trong hệ thống và gửi kết quả báo cáo rà soát về địa chỉ thư điện tử **ncsc@ais.gov.vn chậm nhất trước ngày 25 hàng tháng.**

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: ncsc@ais.gov.vn.

2. Thông tin chi tiết các lỗ hổng

Danh sách lỗ hổng an toàn thông tin đáng chú ý trong các sản phẩm của Microsoft tháng 10/2024

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-43468	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Configuration Manager cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Configuration Manager.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43468
2	CVE-2024-43582	- Điểm CVSS: 8.1 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Remote Desktop Protocol Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43582
3	CVE-2024-43572	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Management Console cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572

4	CVE-2024-43583	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Winlogon cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Thông tin chi tiết về lỗ hổng đã được công bố công khai. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43583
5	CVE-2024-43504	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Excel 2016, 2019. Microsoft Office LTSC 2021, 2024. Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43504
6	CVE-2024-43576 CVE-2024-43616	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office LTSC 2024. Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43576 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43616

7	CVE-2024-43505	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office Visio cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office LTSC 2021, 2024. Microsoft 365 Apps for Enterprise, Microsoft Office 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43505
8	CVE-2024-43573	- Điểm CVSS: 6.5 (Trung bình) - Mô tả: Lỗ hổng trong Windows MSHTML Platform cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43573

3. Khuyến nghị giải pháp

Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng

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.

Kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng an toàn thông tin 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 tham khảo **mục 2** của báo cáo.*

4. Tài liệu tham khảo

https://msrc.microsoft.com/update-guide/

https://www.zerodayinitiative.com/blog/2024/10/8/the-october-2024-security-update-review