Phụ lục

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

(Ban hành kèm theo văn bản số /STTTT-BCVT&CNTT ngày /7/2023 của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-33160 CVE-2023-33134	- Điểm: CVSS: 8.8 (Cao) - Mô tả: lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33160 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33134
2	CVE-2023-36884	- Điểm: CVSS: 8.3 (Cao) - Mô tả: lỗ hổng trong Office và Windows HTML cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, 11, Windows Server, Microsoft Office.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884
3	CVE-2023-35311	- Điểm: CVSS: 8.8 (Cao) - Mô tả: lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). - Ảnh hưởng: Microsoft 365, Microsoft Office, Microsoft Outlook.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35311
4	CVE-2023-36874	- Điểm: CVSS: 7.8 (Cao) - Mô tả: lỗ hổng trong	https://msrc.microsoft.com/update-

ST T	CVE	Mô tả	Link tham khảo
		Windows Error Reporting Service cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server, Windows 10/11.	guide/vulnerability/CVE-2023-36874
5	CVE-2023-32046	- Điểm: CVSS: 7.8 (Cao) - Mô tả: lỗ hổng trong Windows MSHTML cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32046
6	CVE-2023-32049	- Điểm: CVSS: 8.8 (Cao) - Mô tả: lỗ hổng trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32049
7	CVE-2023-32057 CVE-2023-35309	- Điểm: CVSS: 9.8 (Nghiêm trọng) - Mô tả: lỗ hổng trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32057 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35309

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/

https: //www.zerodayinitiative.com/blog/2023/7/10/the-j uly-2023-security-update-review