**Phụ lục**

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

*(Kèm theo Công văn số /CATTT-NCSC ngày / /2023 của Cục An toàn thông tin)*

**1. Thông tin các lỗ hổng bảo mật**

| STT | CVE | Mô tả | Link tham khảo |
|---|---|---|---|
| 1 | CVE-2023-23397 | - Điểm: CVSS: 9.1 (nghiêm trọng)<br>- Mô tả: lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế.<br>- Ảnh hưởng: Microsoft Outlook, Microsoft Office. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397 |
| 2 | CVE-2023-24880 | - Điểm: CVSS: 5.4 (trung bình)<br>- Mô tả: lỗ hổng trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đang bị khai thác trong thực tế.<br>- Ảnh hưởng: Windows Server, Windows 10/11. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24880 |
| 3 | CVE-2023-23392 | - Điểm: CVSS: 9.8 (nghiêm trọng)<br>- Mô tả: lỗ hổng trong HTTP Protocol Stack cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Windows Server, Windows 11. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23392 |
| 4 | CVE-2023-23415 | - Điểm: CVSS: 9.8 (nghiêm trọng)<br>- Mô tả: lỗ hổng trong Internet Control Message Protocol (ICMP) cho phép | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23415 |

| STT | CVE | Mô tả | Link tham khảo |
|---|---|---|---|
| | | đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Windows Server, Windows 10/11. | |
| 5 | CVE-2023-23399 | - Điểm: CVSS: 7.8 (cao)<br>- Mô tả: lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Microsoft Office, Microsoft Excel, Microsoft 365 . | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23399 |
| 6 | CVE-2023-23400 | - Điểm: CVSS: 7.2 (cao)<br>- Mô tả: lỗ hổng trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Windows Server. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23400 |

**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/2023/3/14/the-march-2023-security-update-review