**PHỤ LỤC**

**Thông tin về các lỗ hổng bảo mật trong sản phẩm Microsoft**

*(Kèm theo Công văn số /STTTT-CNTT ngày /8/2022*

*của Sở Thông tin và Truyền thông tỉnh Đắk Lắk)*

**1. Thông tin các lỗ hổng bảo mật**

|  |  |  |  |
| --- | --- | --- | --- |
| **Stt** | **CVE** | **Mô tả** | **Link tham khảo** |
| 1 | CVE-2022-34713 | - Điểm CVSS: 7.8 (Cao)  - Lỗ hổng trong Microsoft Windows Support Diagnostic Tool (MSDT) cho phép đối tượng tấn công thực thi mã từ xa.  - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34713 |
| 2 | CVE-2022-21980  CVE-2022-24477  CVE-2022-24516  CVE-2022-30134 | - Điểm CVSS: 8.0 (Cao)  - Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thu thập thông tin và thực hiện leo thang đặc quyền.  - Ảnh hưởng: Microsoft Exchange Server 2013/2016/2019. | <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21980>  <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24477>  <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24516>  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30134 |
| 3 | CVE-2022-35804 | - Điểm CVSS: 8.8 (Cao)  - Lỗ hổng trong SMB Client and Server cho phép đối tượng tấn công chưa xác thực có thể thực thi mã từ xa.  - Ảnh hưởng: Windows 11. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35804 |
| 4 | CVE-2022-34715 | - Điểm CVSS: 9.8 (Nghiêm trọng)  - Lỗ hổng trong Windows Network File System cho phép đối tượng tấn công chưa xác thực có thể thực thi mã từ xa.  - Ảnh hưởng: Windows Server 2022. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34715 |
| 5 | CVE-2022-35742 | - Điểm CVSS: 7.5 (Cao)  - Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ.  - Ảnh hưởng: Microsoft Outlook 2012/2016, Microsoft Office LTSC 2021/2019, Microsoft 365 Apps. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35742 |

**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. Các cơ quan, 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 này.

**3. Tài liệu tham khảo**

https://msrc.microsoft.com/update-guide/releaseNote/2022-Aug

https://www.zerodayinitiative.com/blog/2022/8/9/the-august-2022-security-update-review