|  |  |
| --- | --- |
| UBND TỈNH TÂY NINH  **SỞ THÔNG TIN VÀ TRUYỀN THÔNG**  Số: /STTTT-TTGSĐH  Về việc cảnh báo lỗ hổng bảo mật Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 6/2022. | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**  **Độc lập – Tự do – Hạnh phúc**  *Tây Ninh, ngày tháng 6 năm 2022* |

Kính gửi:

- Văn phòng Tỉnh ủy;

- Văn phòng Đoàn ĐBQH và HĐND tỉnh;

- Văn phòng UBND tỉnh;

- Các cơ quan tham mưu, giúp việc Tỉnh ủy;

- Mặt trận Tổ quốc và các Đoàn thể chính trị - xã hội;

- Các Sở, ban, ngành tỉnh;

- Các huyện, thị, thành ủy;

- UBND các huyện, thị xã, thành phố.

Thực hiện theo Công văn số 869/CATTT-NCSC ngày 16/6/2022 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc cảnh báo lỗ hổng bảo mật Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 6/2022 *(Chi tiết lỗ hổng trong phụ lục kèm theo).*

Nhằm đảm bảo an toàn thông tin cho người dùng, đơn vị và toàn bộ hệ thống của tỉnh, Sở Thông tin và Truyền thông đề nghị các đơn vị, địa phương thực hiện gấp các công việc cụ thể như sau:

1. Kiểm tra, xác định các thiết bị máy tính sử dụng hệ điều hành Windows, phần mềm ứng dụng liên quan có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời theo hướng dẫn tại phụ lục để tránh nguy cơ bị tấn công.
2. Tăng cường kiểm tra, giám sát và sẵn sàng phương án 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.

Thông tin liên quan đề nghị liên hệ Ông Vương Duy Thanh - Trung tâm Giám sát, điều hành kinh tế, xã hội tập trung; Điện thoại: 0932624462.

Trân trọng./.

|  |  |
| --- | --- |
| ***Nơi nhận:***  - Như trên;  - GĐ Sở (b/c);  - P. CNTTBCVT;  - Lưu: VT, TTGSĐH. | **KT. GIÁM ĐỐC**  **PHÓ GIÁM ĐỐC** |

# PHỤ LỤC

# THÔNG TIN CÁC LỖ HỔNG BẢO MẬT CAO VÀ NGHIÊM TRỌNG TRONG CÁC SẢN PHẨM MICROSOFT CÔNG BỐ THÁNG 6/2022

1. **Thông tin về các lỗ hổng:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Stt** | **Mã lỗ hổng** | **Mô tả** | **Tham khảo** |
| 1 | CVE-2022-30190 (Follina) | * Điểm CVSS: 7.8 (Cao) * Lỗ hổng trong Windows Microsoft Support Diagnostic Tool (MSDT) cho phép đối tượng tấn công thực thi mã tùy ý. * Ảnh hưởng: Windows 7/8.1/10, Windows Server 2008/2012/2016. | <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190>  Văn bản số 786/CATTT-NCSC về việc lỗ hổng bảo mật CVE-2022-30190 trong Microsoft Support Diagnostic Tool phát hành ngày 01/6/2022. |
| 2 | CVE-2022-30136 | * Điểm CVSS: 9.8 (Nghiêm trọng) * Lỗ trong Windows Network File System cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa. * Ảnh hưởng: Windows Server 2012/2016/2019. | <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30136> |
| 3 | CVE-2022-30163 | * Điểm CVSS: 8.5 (Cao) * Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa. * Ảnh hưởng: Windows 8.1/10/11, Windows Server 2008/2012/2016. | <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30163> |
| 4 | CVE-2022-30139 | * Điểm CVSS:7.5 (cao). * Lỗ hổng trong Windows Lightweight Directory Access Protocol (LDAP) cho phép đối tượng tấn công thực thi mã từ xa. * Ảnh hưởng: Windows 10, Windows Server 2016/2019/2022 | [CVE-2022-30139 - Security Update Guide - Microsoft - Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30139) |
| 5 | CVE-2022-30157  CVE-2022-30158 | * Điểm CVSS: 8.8 (Cao) * Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. * Ảnh hưởng: SharePoint Server 2019, SharePoint Enterprise Server 2016. | [CVE-2022-30157 - Security Update Guide - Microsoft - Microsoft SharePoint Server Remote Code Execution Vulnerability](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30157) |
| 6 | CVE-2022-30165 | * Điểm CVSS: 8.8 (Cao) * Lỗ hổng trong Windows Kerberos cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. * Ảnh hưởng: Windows 10/11, Windows Server 2016/2022. | [https://msrc.microsoft.com/update-guide/vulnerability/CV E-2022-30165](https://msrc.microsoft.com/update-guide/vulnerability/CV%20E-2022-30165) |
| 7 | CVE-2022-30173 | * Điểm CVSS: 7.8 (Cao) * Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. * Ảnh hưởng: Excel 2013/2016 | [https://msrc.microsoft.com/update-guide/vulnerability/CV E-2022-30173](https://msrc.microsoft.com/update-guide/vulnerability/CV%20E-2022-30173) |
| 8 | C VE-2022-30174 | * Điểm CVSS: 7.4 (Cao) * Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. * Ảnh hưởng: Microsoft 365 Apps, Microsoft Office LTSC 2021. | [https://msrc.microsoft.com/update-guide/vulnerability/CV E-2022-30174](https://msrc.microsoft.com/update-guide/vulnerability/CV%20E-2022-30174) |

1. **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 phụ lục trên.

1. **Tài liệu tham khảo:**

[June 2022 Security Updates - Release Notes - Security Update Guide - Microsoft](https://msrc.microsoft.com/update-guide/releaseNote/2022-Jun)

[Zero Day Initiative — The June 2022 Security Update Review](https://www.zerodayinitiative.com/blog/2022/6/14/the-june-2022-security-update-review)