UBND TỈNH LÂM ĐỒNG
**SỞ THÔNG TIN VÀ TRUYỀN THÔNG**

Số: 436 /STTTT-TTTHDL&CĐS
V/v lỗ hổng bảo mật trong các sản phẩm Microsoft công bố tháng 04/2023 và cảnh báo đơn vị có IP nằm trong mạng Botnet tháng 04/2023

**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM**
**Độc lập - Tự do - Hạnh phúc**

*Lâm Đồng, ngày 24 tháng 04 năm 2023*

Kính gửi:
- Văn phòng Tỉnh ủy;
- Văn phòng UBND tỉnh;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Các Sở, Ban, Ngành;
- Công an tỉnh;
- Bộ Chỉ huy quân sự tỉnh;
- Thành ủy, huyện ủy, UBND các huyện, thành phố.

Ngày 11/04/2023, Microsoft đã phát hành danh sách bản vá tháng 04 với 97 lỗ hổng bảo mật trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý các lỗ hổng bảo mật có mức ảnh hưởng cao và nghiêm trọng sau:

- Lỗ hổng bảo mật **CVE-2023-28252** trong Windows Common Log File System Driver cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế.

- Lỗ hổng bảo mật **CVE-2023-21554** trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa.

- 03 lỗ hổng bảo mật **CVE-2023-23384, CVE-2023-23375, CVE-2023-28304** trong Microsoft SQL Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2013-3900** xác thực chữ ký WinVerifyTrust cho phép đối tượng tấn công có thể thêm nội dung vào phần chữ ký mã xác thực trong tệp thực thi đã ký mà không làm mất hiệu lực chữ ký. Gần đây, lỗ hổng này đã được sử dụng trong các cuộc tấn công chuỗi cung ứng vào phần mềm của hãng 3CX. Microsoft đã đưa ra bản vá về việc kiểm tra tính xác thực của chữ ký dưới dạng tùy chọn bật hoặc tắt, nếu không được cấu hình sẽ mặc định là tắt. Trong bản cập nhật này Microsoft đã bổ sung thêm các phiên bản hệ điều hành bị ảnh hưởng. Để nâng cao bảo mật an toàn thông tin cho các thiết bị sử dụng hệ điều hành Windows người dùng có thể xem xét việc bật tùy chọn kiểm tra này.

- 02 lỗ hổng bảo mật **CVE-2023-28287, CVE-2023-28295** trong Microsoft Publisher cho phép đối tượng tấn công thực thi mã từ xa.

- 02 lỗ hổng bảo mật **CVE-2023-28309, CVE-2023-28314** trong Microsoft Dynamics 365 cho phép đối tượng tấn công thực hiện tấn công XSS *(Thông tin chi*

*tiết các lỗ hổng bảo mật có tại phụ lục kèm theo).*

- Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan nhà nước trên địa bàn tỉnh, Sở Thông tin và Truyền thông tỉnh Lâm Đồng đề nghị các cơ quan, đơn vị tiếp tục kiểm tra, rà soát, xác định các máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. (*Tham khảo thông tin tại phụ lục kèm theo*).

- Tăng cường giám sát và sẵn sàng phương án xử lý 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.

- Kiểm tra, rà soát, tháo gỡ mã độc tồn tại trong mạng nội bộ các đơn vị có IP Public nằm trong mạng Botnet do Trung tâm Giám sát an toàn không gian mạng quốc gia (National Cyber Security Center - NCSC) cung cấp (*có danh sách đính kèm*).

**Trong trường hợp cần hỗ trợ, xin vui lòng liên hệ:**

- Ông Nguyễn Xuân Tùng - Phó phòng CNTT - Điện thoại: 0263.3541542, Di động: 0975886197.

- Ông Phan Minh Hoàng - Trung tâm tích hợp dữ liệu và Chuyển đổi số - Điện thoại: 0984497451./.

***Nơi nhận:***
- Như trên;
- GĐ Sở (b/c);
- Phòng VHTT các huyện, thành phố;
- Đội ứng cứu sự cố mạng, máy tính tỉnh Lâm Đồng;
- Lưu: VT, TT THDL&CĐS.

**KT. GIÁM ĐỐC**
**PHÓ GIÁM ĐỐC**

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH LÂM ĐỒNG

**Lê Thanh Liêm**

**Phụ lục 1**
**Thông tin về các lỗ hổng bảo mật trong sản phẩm Microsoft**
*(Kèm theo Công văn Số: /STTTT-TTTHDL&CĐS ngày / 04 /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-2023-28252 | - Điểm: CVSS: 7.8 (cao)<br>- Mô tả: lỗ hổng trong Windows Common Log File System Driver 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: Windows Server, Windows 10,11. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28252 |
| 2 | CVE-2023-21554 | - Điểm: CVSS: 9.8 (nghiêm trọng)<br>- Mô tả: lỗ hổng trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Windows Server, Windows 10/11. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21554 |
| 3 | CVE-2023-23384<br>CVE-2023-23375<br>CVE-2023-28304 | - Điểm: CVSS: 7.8/7.3 (cao)<br>- Mô tả: lỗ hổng trong Microsoft SQL Server cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Microsoft SQL Server, Microsoft ODBC Driver 18. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23384<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23375<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28304 |
| 4 | CVE-2013-3900 | - Điểm: CVSS: 7.4 (cao)<br>- Mô tả: lỗ hổng xác thực chữ ký WinVerifyTrust cho phép đối tượng tấn công có thể thêm nội dung vào phần chữ ký mã xác | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900 |

| | | | |
|---|---|---|---|
| | | thực trong tệp thực thi đã ký mà không làm mất hiệu lực chữ ký.<br>- Ảnh hưởng: Windows Server, Windows 10/11. | |
| 5 | CVE-2023-28287<br>CVE-2023-28295 | - Điểm: CVSS: 8.8 (cao)<br>- Mô tả: lỗ hổng trong Microsoft Publisher cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Microsoft Office, Microsoft Publisher. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28287<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28295 |
| 6 | CVE-2023-28309<br>CVE-2023-28314 | - Điểm: CVSS: 7.6/6.1 (cao)<br>- Mô tả: lỗ hổng trong Microsoft Dynamics 365 cho phép đối tượng tấn công thực hiện tấn công XSS.<br>- Ảnh hưởng: Microsoft Dynamics 365. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28309<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28314 |

**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/2023/4/11/the-april-2023-security-update-review

**Phụ lục 2**

**THÔNG TIN VỀ CÁC ĐƠN VỊ CÓ IP NẰM TRONG MẠNG BOTNET THÁNG 04/2023**

*(Kèm theo Công văn Số: /STTTT-TTTHDL&CĐS ngày / 04 /2023 của Sở Thông tin và Truyền thông)*

| THÔNG TIN VỀ CÁC ĐƠN VỊ CÓ IP NẰM TRONG MẠNG BOTNET | | | |
|---|---|---|---|
| **STT** | **IP** | **Tên đơn vị** | **C&C server** |
| 1 | 113.161.184.14 | UBND Phường 2 Đà lạt | 63.251.126.11 |
| 2 | 113.161.184.187 | Thanh tra tỉnh | 184.105.192.2 |
| 3 | 113.165.166.72 | UBND huyện Đức Trọng | 63.251.126.11 |
| 4 | 113.165.166.109 | UBND huyện Cát tiên | 173.231.189.17 |
| 5 | 113.164.94.114 | Sở Tài chính | 216.218.135.118<br>184.105.192.2 |
| 6 | 113.165.167.92 | Văn phòng Đoàn ĐBQH và HĐND tỉnh | 184.105.192.2 |
| 7 | 113.165.166.150 | UBND huyện Lạc Dương | 208.100.26.245 |
| 8 | 113.164.94.179 | UBND Tp. Bảo Lộc | 184.105.192.2 |