UBND TỈNH NAM ĐỊNH
**SỞ THÔNG TIN VÀ TRUYỀN THÔNG**

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

Số:44 /STTTT-CNTT

*Nam Định, ngày 17 tháng 01 năm 2022*

V/v kiểm tra, rà soát và khắc phục lỗ hổng bảo mật mới mức cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2022

Kính gửi:
- Các sở, ban, ngành của tỉnh;
- UBND các huyện, thành phố;
- VNPT Nam Định;
- Viettel Nam Định.

Căn cứ Văn bản số 56/CATTT-NCSC ngày 12/01/2022 của Cục An toàn thông tin vê việc cảnh báo lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2022.

Theo đó, ngày 11/01/2022, Microsoft đã phát hành danh sách bản vá tháng 1 với 96 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 sau:

**** Các lỗ hổng có mức ảnh hưởng Nghiêm trọng:***

- Lỗ hổng bảo mật **CVE-2022-21907** trong HTTP Protocol Stack (http.sys) của Windows, cho phép đối tượng tấn công thực thi mã từ xa mà không cần xác thực.

**** Các lỗ hổng có mức ảnh hưởng Cao:***

- 03 lỗ hổng bảo mật **CVE-2022-21846, CVE-2022-21969, CVE-2022-21855** trong Microsoft Exchange Server, cho phép đối tượng tấn công thực thi mã từ xa. Để khai thác lỗ hổng này, kẻ tấn công cần có quyền truy cập vào mạng mục tiêu từ đấy có thể chiếm quyền điều khiển máy chủ.
- Lỗ hổng bảo mật **CVE-2022-21857** trong Active Directory, cho phép đối tượng nâng cao đặc quyền.
- Lỗ hổng bảo mật **CVE-2022-21840** trong Microsoft Office, cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng bảo mật **CVE-2022-21911** trong .NET Framework, cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ.
- Lỗ hổng bảo mật **CVE-2022-21836** trong Windows Certificate, cho phép đối tượng tấn công giả mạo.
- Lỗ hổng bảo mật **CVE-2022-21841** trong Microsoft Excel, cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng bảo mật **CVE-2022-21837** trong Microsoft SharePoint Server, cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng bảo mật **CVE-2022-21842** trong Microsoft Word, cho phép đối tượng tấn công thực thi mã từ xa.

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, doanh nghiệp trên địa bàn tỉnh, Sở Thông tin và Truyền thông đề nghị các sở, ban, ngành của tỉnh; UBND các huyện, thành phố và VNPT Nam Định, Viettel Nam Định phối hợp triển khai thực hiện một số nội dung sau:

1. Đề nghị các sở, ban, ngành của tỉnh; UBND các huyện, thành phố:

- Kiểm tra, rà soát và xác định máy chủ, máy trạm sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công (tham khảo thông tin tại phụ lục kèm theo).

- Chỉ đạo, hướng dẫn, hỗ trợ các đơn vị trực thuộc và UBND các xã, phường, thị trấn tổ chức triển khai thực hiện nội dung trên.

- Tăng cường giám sát và kịp thời thông báo về Sở Thông tin và Truyền thông khi phát hiện có dấu hiệu bị khai thác, tấn công mạng.

2. Đề nghị VNPT Nam Định, Viettel Nam Định thực hiện việc rà soát, kiểm tra, cập nhật bản vá cho máy tính, thiết bị trong hệ thống thông tin đang cung cấp các dịch vụ, phần mềm cho các cơ quan nhà nước trên địa bàn tỉnh.

3. Yêu cầu Trung tâm Công nghệ thông tin và Truyền thông:

- Thực hiện rà soát, kiểm tra; cập nhật bản vá bảo mật cho các máy bị ảnh hưởng đối với các máy tính, thiết bị tại Trung tâm Tích hợp dữ liệu của tỉnh.

- Làm đầu mối hỗ trợ, hướng dẫn các sở, ban, ngành của tỉnh; UBND các huyện, thành phố xử lý, khắc phục lỗ hổng.

- Chủ động triển khai các giải pháp và phối hợp với Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin kịp thời xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng, đảm bảo an toàn thông tin tại Trung tâm Tích hợp dữ liệu của tỉnh.

Sở Thông tin và Truyền thông đề nghị các Sở, ban, ngành của tỉnh; UBND các huyện, thành phố và VNPT Nam Định, Viettel Nam Định quan tâm phối hợp triển khai thực hiện.

Thông tin liên hệ: Đầu mối hỗ trợ kỹ thuật: ông Trần Tuấn Anh, Kỹ sư Trung tâm CNTT&TT (số điện thoại: 0376805976, email: trantuananh.stt@namdinh.gov.vn); Đầu mối tổng hợp: ông Phạm Văn An, Chuyên viên Phòng Công nghệ thông tin (điện thoại: 0949268749, email: phamvanan.stt@namdinh.gov.vn).

Trân trọng./.

***Nơi nhận:***
- Như trên;
- Trung tâm CNTT&TT (để thực hiện);
- Lưu: VT, CNTT (anpv).

**GIÁM ĐỐC**

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH NAM ĐỊNH

**Vũ Trọng Quế**

**Phụ lục**

**Thông tin lỗ hổng bảo mật**

*(Kèm theo Công văn số /STTTT-CNTT ngày /01/2022 của Sở Thông tin và Truyền thông)*

**1. Thông tin các lỗ hổng bảo mật**

| STT | CVE | Mô tả | Link tham khảo |
|---|---|---|---|
| 1 | CVE-2022-21907 | - Điểm CVSS: 9.8 (Nghiêm trọng)<br>- Lỗ hổng trong HTTP Protocol, cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Windows Server 2019/2022, Windows 11/10. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21907 |
| 2 | CVE-2022-21846 | - Điểm CVSS: 9.0 (Cao)<br>- Lỗ hổng trong Exchange Server, cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Microsoft Exchange Server 2019/2016/2013. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21846 |
| 3 | CVE-2022-21855 | - Điểm CVSS: 9.0 (Cao)<br>- Lỗ hổng trong Exchange Server, cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Microsoft Exchange Server 2019/2016/2013. | https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21855 |
| 4 | CVE-2022-21969 | - Điểm CVSS: 9.0 (Cao)<br>- Lỗ hổng trong Exchange Server, cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Microsoft Exchange Server 2019/2016/2013. | https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21969 |

| | | | |
|---|---|---|---|
| 5 | CVE-2022-21840 | - Điểm CVSS: 8.8 (Cao)<br>- Lỗ hổng trong Microsoft Office, cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Microsoft SharePoint Foundation 2013, SharePoint Server 2019, Microsoft Office 2016/2013/LTSC 2021/2019, Microsoft Excel 2016/2013, Microsoft 365 | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21840 |
| 6 | CVE-2022-21875 | - Điểm CVSS: 8.8 (Cao)<br>- Lỗ hổng trong Active Directory Domain Services, cho phép đối tượng tấn công nâng cao đặc quyền.<br>- Ảnh hưởng: Windows Server 2022/2019/2016/2012/2008, Windows 11/10/RT 8.1/7. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21857 |
| 7 | CVE-2022-21911 | - Điểm CVSS: 7.5 (Cao)<br>- Lỗ hổng trong .NET Framework, cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ.<br>- Ảnh hưởng: Microsoft .NET Framework 3.5 AND 4.7.2, 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2,… | https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21911 |
| 8 | CVE-2022-21836 | - Điểm CVSS: 7.8 (cao)<br>- Lỗ hổng trong Windows Certificate, cho phép đối tượng tấn công thực hiện tấn công giả mạo<br>- Ảnh hưởng: Windows Server 2022/2019/2016/2012/2008, Windows 10/RT 8.1/7. | https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21836 |

| | | | |
|---|---|---|---|
| 9 | CVE-2022-21841 | - Điểm CVSS: 7.8 (cao)<br>- Lỗ hổng trong Microsoft Excel, cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Microsoft Office 2013/2016/2019/LTSC2021, Microsoft 365. | https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21841 |
| 10 | CVE-2022-21837 | - Điểm CVSS: 8.3 (cao)<br>- Lỗ hổng trong Microsoft SharePoint Server, cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Microsoft SharePoint Server 2019, 2016 | https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21837 |
| 11 | CVE-2022-21842 | - Điểm CVSS: 7.8 (cao)<br>- Lỗ hổng trong Microsoft Word, cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Microsoft Word 2016. | https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21842 |

**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/releaseNote/2022-Jan
https://msrc.microsoft.com/update-guide/en-us