SỞ THÔNG TIN VÀ TRUYỀN THÔNG
THANH HÓA
TRUNG TÂM CNTT&TT

Số: 151 /TTCNTT&TT-QTHT
V/v lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 10/2022

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

Thanh Hoá, ngày 17 tháng 10 năm 2022

Kính gửi:
- Văn Phòng Tỉnh ủy;
- Văn Phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn Phòng UBND tỉnh;
- Các Sở, ban, ngành cấp tỉnh;
- UBND các huyện, thị xã, thành phố;
- Các cơ quan đoàn thể chính trị cấp tỉnh;
- Các doanh nghiệp VT-CNTT trên địa bàn tỉnh.

Căn cứ Công văn số 1559/CATTT-NCSC ngày 13/10/2022 của Cục An toàn thông tin, Bộ Thông tin và Truyền thông về lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 10/2022. Theo đó, ngày 11/10/2022, hãng Microsoft đã phát hành danh sách bản vá tháng 10 với 85 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-2022-41033** trong Windows COM + Event System Service cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã được một số nhóm tấn công khai thác trong thực tế.

- 02 lỗ hổng bảo mật **CVE-2022-37987, CVE-2022-37989** trong Windows Client Server Run-time Subsystem (CSRSS) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-37968** trong Azure Arc-enabled Kubernetes cluster Connect cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

- 03 lỗ hổng bảo mật **CVE-2022-38048, CVE-2022-41043, CVE-2022-38001** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa, thu thập thông tin, tấn công giả mạo (Spoofing). Trong đó lỗ hổng CVE-2022-41043 đã được công bố rộng rãi trên Internet.

- 03 lỗ hổng bảo mật **CVE-2022-41036, CVE-2022-41037, CVE-2022-41038** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-41031** trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-37976** trong Active Directory Certificate Services cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

(Thông tin chi tiết các lỗ hổng bảo mật có tại phụ lục kèm theo)

Để tăng cường chủ động phòng ngừa các rủi ro mất an toàn thông tin tại các hệ thống thông tin của các cơ quan đơn vị, với chức năng và nhiệm vụ bảo đảm an toàn thông tin mạng trên địa bàn tỉnh được Chủ tịch UBND tỉnh, Giám đốc Sở Thông tin và Truyền thông giao, Trung tâm Công nghệ thông tin và Truyền thông, đề nghị các cơ quan, địa phương trên địa bàn tỉnh chỉ đạo các bộ phận, cá nhân liên quan thực hiện tốt các nội dung sau:

1. Kiểm tra, rà soát, xác định máy 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. Hướng dẫn kỹ thuật cách thức thực hiện chi tiết đối với lỗ hổng bảo mật tại địa chỉ: *https://attt.thanhhoa.gov.vn*.

2. 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.

Trong quá trình thực hiện, nếu gặp khó khăn, vướng mắc về kỹ thuật liên quan đến các nội dung, công việc trên đề nghị liên hệ với Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa (cơ quan thường trực của Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh) để phối hợp xử lý.

Điện thoại: (0237).3718.699

Hộp thư điện tử tiếp nhận báo cáo sự cố: ungcuusuco@thanhhoa.gov.vn

Xin trân trọng cảm ơn./.

Nơi nhận:
- Như kính gửi;
- Sở TT&TT (để b/c);
- PGĐ Sở Nguyễn Văn Tước (để b/c);
- Giám đốc Trung tâm (để b/c);
- Lưu: VT, QTHT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

SỞ THÔNG TIN VÀ TRUYỀN THÔNG TỈNH THANH HÓA
TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Trần Ngọc Hưng

Phụ lục: Thông tin các lỗ hổng bảo mật
(Kèm theo công văn số /TTCNTT&TT-QTHT ngày tháng năm 2022 của Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Địa chỉ tham khảo
1	CVE-2022-41033	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows COM + Event System Service cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã được một số nhóm tấn công khai thác trong thực tế. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41033
2	CVE-2022-37987 CVE-2022-37989	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong trong Windows Client Server Run-time Subsystem (CSRSS) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37987 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37989
3	CVE-2022-37968	- Điểm CVSS: 10 (Nghiêm trọng) - Lỗ hổng trong Azure Arc-enabled Kubernetes cluster Connect cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Azure Stack Edge, Azure Arc-enabled Kubernetes cluster 1.6.19/1.5.8/1.7.18/1.8.11	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37968
4	CVE-2022-38048 CVE-2022-41043 CVE-2022-38001	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong trong Microsoft Office cho phép	https://msrc.microsoft.com/update-guide/vulnerability/CV

STT	CVE	Mô tả	Địa chỉ tham khảo
		đối tượng tấn công thực thi mã từ xa, thu thập thông tin, tấn công giả mạo (Spoofing). - Ảnh hưởng: Microsoft Office 2013/2016/2019, Office 365 Apps, Office LTSC.	E-2022-38048 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41043 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38001
5	CVE-2022-41036 CVE-2022-41037 CVE-2022-41038	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server 2016/2019, SharePoint Foundation/Enterprise Server 2013.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41036 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41037 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41038
6	CVE-2022-41031	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft 365 Apps, Microsoft Office 2019/LTSC.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41031
7	CVE-2022-37976	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Active Directory Certificate Services cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/ 2022	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37976

2. Hướng dẫn khắc phục

Hướng dẫn chi tiết khắc phục các lỗ hổng bảo mật trên tại địa chỉ: **https://attt.thanhhoa.gov.vn** (*Mục Hướng dẫn → Kỹ năng An toàn thông tin*)

3. Tài liệu tham khảo

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

https://www.zerodayinitiative.com/blog/2022/10/11/the-october-2022-security-update-review