UỶ BAN NHÂN DÂN **PHƯỜNG BẠCH SAM**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 119 /UBND-VHXH	*Bạch Sam, ngày 21 tháng 5 năm 2024*

V/v cảnh báo chiến dịch tấn công mới nhằm vào các thiết bị mạng Cisco

Kính gửi: Các ngành, đoàn thể, CBCC phường.

Theo thông báo của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về cảnh báo phát hiện mã độc tấn công mạng ArcaneDoor ảnh hưởng đến các thiết bị mạng Cisco. Khi truy cập được vào các thiết bị này, đối tượng tấn công có thể điều hướng lại hoặc điều chỉnh lưu lượng mạng, theo dõi liên lạc trong mạng lưới và thực hiện hành động trái phép.

Trong thời gian vừa qua, đã cho thấy sự gia tăng của các chiến dịch tấn công nhằm vào thiết bị mạng trong lĩnh vực cung cấp dịch vụ viễn thông và tổ chức năng lượng. Thông qua quá trình điều tra phân tích, các nhà phân tích thấy rằng các nhóm tấn công thường triển khai mã độc, thực thi mã từ xa trên thiết bị bị ảnh hưởng. Hai lỗ hổng bị khai thác gồm có:

- CVE-2024-20353 (Điểm CVSS: 8.6 - Cao) tồn tại trên Cisco Adaptive Security Appliance (ASA) Software và Cisco Firepower Threat Defense (FTD) Software cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ.

- CVE-2024-20359 (Điểm CVSS: 6.0 - Trung bình) tồn tại trên Cisco Adaptive Security Appliance (ASA) Software và Cisco Firepower Threat Defense (FTD) Software cho phép đối tượng tấn công thực thi mã tùy ý với đặc quyền root.

Thực hiện Công văn số 566/STTTT-BCVTCNTT ngày 06/5/2024 của Sở Thông tin và Truyền thông tỉnh Hưng Yên; Công văn số 761/UBND-VHTT ngày 15/5/2024 của UBND thị xã Mỹ Hào về cảnh báo chiến dịch tấn công mới nhằm vào các thiết bị mạng Cisco.

Để bảm bảo an toàn thông tin cho hệ thống thông tin đang được sử dụng tại các Ngành, đoàn thể, CBCC trên địa bàn phường. UBND phường yêu cầu Thủ trưởng các ngành, đoàn thể, CBCC phường triển khai thực hiện rà soát, khắc phục lỗ hổng bảo mật trên theo khuyến nghị sau:

1. Thực hiện kiểm tra, rà soát các các hệ thống, thiết bị đang sử dụng có khả năng bị ảnh hưởng bởi lỗ hổng trên. Thực hiện nâng cấp lên phiên bản mới nhất để tránh nguy cơ bị tấn công (*tham khảo hướng dẫn gửi kèm Công văn*).

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.

3. Trong trường hợp cần hỗ trợ Trưởng các ngành, đoàn thể, CBCC phường liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại: 02432.091.616, thư điện tử: ais@mic.gov.vn; Sở Thông tin và Truyền thông (đồng chí Đặng Xuân Dương, số điện thoại: 0988.283.898).

UBND phường yêu cầu Trưởng các ngành, đoàn thể, CBCC phường nghiêm túc triển khai thực hiện./.

Nơi nhận:
- Như kính gửi;
- Chủ tịch, Phó Chủ tịch UBND phường;
- Các ngành, đoàn thể, CBCC phường;
- Lưu: VP, VHXH.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

U.B.N.D PHƯỜNG BẠCH SAM TỈNH HƯNG YÊN

Ký bởi: Ủy ban nhân dân phường Bạch Sam
Cơ quan: Tỉnh Hưng Yên
Thời gian ký: 21/05/2024 18:41:17

Phạm Ngọc Chiến