UBND TỈNH NINH THUẬN
SỞ Y TẾ
Số: 1903 /SYT-KHNVTC

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

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

Ninh Thuận, ngày10 tháng 5 năm 2024

Kính gửi: Các đơn vị trực thuộc.

Tiếp nhận Công văn số 1098/STTTT-TTCNTT&TT ngày 04/5/2024 của Sở Thông tin và Truyền thông về Cảnh báo chiến dịch tấn công mới nhằm vào các thiết bị mạng Cisco.

Qua công tác giám sát an toàn không gian mạng quốc gia, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin - Bộ Thông tin và Truyền thông, ghi nhận chiến dịch 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 hoặc điều chỉnh lưu lượng mạng, theo dõi liên lạc trong mạng và thực hiện hành động trái phép.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Y tế yêu cầu các đơn vị thực hiện:

1. Kiểm tra, rà soát hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi chiến dịch tấn công trên. Chủ động theo dõi các thông tin liên quan đến chiến dịch tấn công mạng, sẵn sàng các biện pháp bảo mật để tránh nguy cơ bị tấn công. *(Tham khảo thông tin tại Phụ lục kèm theo)*

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 được hỗ trợ các cơ quan, đơn vị liên hệ Trung tâm Giám sát an toàn, an ninh, thông tin mạng (qua tổng đài điện thoại 1022 hoặc thư điện tử: ioc@ninhthuan.gov.vn).

Sở Y tế thông báo và yêu cầu các đơn vị triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Lãnh đạo Sở;
- Website Sở Y tế;
- Lưu: VT, KHNVTC.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ Y TẾ
TỈNH NINH THUẬN

Bùi Văn Kỳ

Phụ lục
THÔNG TIN CHI TIẾT
(Kèm theo Công văn số /SYT-KHNVTC ngày / /2024 của Sở Y tế)

1. Thông tin chi tiết về chiến dịch tấn công

Chiến dịch 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. Vào đầu năm 2024, trong một cuộc điều tra phân tích đã phát hiện được một nhóm tấn công mới hiện đang được theo dõi dưới tên UAT4356 bởi Talos và STORM-1849 bởi Microsoft Threat Intelligence Center.

Được biết UAT4356 đã triển khai hai backdoor trong chiến dịch lần này, có tên "Line Runner" và "Line Dance", cả hai được sử dụng để thực hiện các hành vi độc hại lên thiết bị bị ảnh hưởng, bao gồm: điều chỉnh cấu hình, do thám, theo dõi/trích xuất lưu lượng mạng và leo thang đặc quyền.

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.

Các đơn vị có thể tải xuống các mã IOC tại https://alert.khonggianmang.vn/

Dưới đây là một số IoC được ghi nhận

192.36.57[.]181	185.167.60[.]85
185.227.111[.]17	176.31.18[.]153
172.105.90[.]154	185.244.210[.]120
45.86.163[.]224	172.105.94[.]93
213.156.138[.]77	89.44.198[.]189
45.77.52[.]253	103.114.200[.]230
212.193.2[.]48	51.15.145[.]37
89.44.198[.]196	131.196.252[.]148
213.156.138[.]78	121.227.168[.]69
213.156.138[.]68	194.4.49[.]6
185.244.210[.]65	216.238.75[.]155

2. Khuyến nghị:

- Kiểm tra lại các thiết bị mạng đồng thời thực hiện cập nhật bản vá mới nhất

- Ghi chép lại sự kiện của thiết bị vào một địa điểm bảo mật tập trung.

- Sử dụng xác thực đa bước (MFA) bảo mật cao.

3. Tài liệu tham khảo

https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/