

Số: /CATTT-NCSC
V/v Cảnh báo chiến dịch tấn công mới
nhằm vào các thiết bị mạng Cisco

Hà Nội, ngày tháng năm 2024

Kính gửi:

- Đơn vị chuyên trách về CNTT/ATTT các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước;
- Các Doanh nghiệp cung cấp dịch vụ viễn thông, Internet và nền tảng số;
- Các Tổ chức tài chính, Ngân hàng thương mại;
- Hệ thống các đơn vị chuyên trách về an toàn thông tin.

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.

(Thông tin chi tiết xem tại Phụ lục kèm theo)

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý Đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Cục An toàn thông tin khuyến nghị Quý 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.
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 thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ncsc@ais.gov.vn.

Trân trọng./.

Nơi nhận:

- Như trên;
- Thứ trưởng Phạm Đức Long (đề b/c);
- Cục A05 (Bộ Công an);
- Bộ Tư lệnh 86 (Bộ Quốc phòng);
- Ban Cơ yếu Chính phủ;
- Đơn vị chuyên trách về CNTT/ATTT của: Văn phòng Trung ương Đảng; Văn phòng Quốc hội; Văn phòng Chủ tịch nước; Tòa án nhân dân tối cao; Viện Kiểm sát nhân dân tối cao; Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam;
- Các Cục: Viễn thông, Bưu điện Trung ương;
- Trung tâm VNNIC, Trung tâm Thông tin;
- Các Tập đoàn kinh tế và Tổng công ty nhà nước;
- Các Tổ chức tài chính, Ngân hàng thương mại nhà nước;
- Ngân hàng Chính sách xã hội;
- Ngân hàng Phát triển Việt Nam;
- Ngân hàng Hợp tác xã Việt Nam;
- Các Tổ chức, doanh nghiệp hoạt động trong lĩnh vực thương mại điện tử;
- Các tổ chức, doanh nghiệp cung cấp dịch vụ trung gian thanh toán, ví điện tử;
- Cục trưởng (đề b/c);
- Các Phó Cục trưởng;
- P.ATHTTT, P.QHPT, VNCERT/CC;
- Lưu: VT, NCSC.LTQ.

**KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG**

Trần Đăng Khoa

Phụ lục
THÔNG TIN CHI TIẾT
(Kèm theo Công văn số /CATTT-NCSC ngày / /2024
của Cục An toàn thông tin)

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 của doanh nghiệp, tổ chức 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/>