

UBND TỈNH QUẢNG NGÃI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: /STTTT-BCVT&CNTT

Quảng Ngãi, ngày tháng 5 năm 2024

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

Kính gửi:

- Văn phòng: Tỉnh ủy, Đoàn ĐBQH&HĐND, UBND tỉnh;
- Các sở, ban, ngành; Hội, đoàn thể tỉnh;
- UBND các huyện, thị xã, thành phố;
- Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Công an tỉnh;
- Báo Quảng Ngãi, Đài Phát thanh và Truyền hình tỉnh;
- UBND các xã, phường, thị trấn.

Theo cảnh báo của Cục An toàn thông tin tại Công văn số 764/CATTT-NCSC ngày 03/5/2024 về cảnh báo chiến dịch tấn công mới nhằm vào các thiết bị mạng CISCO, Sở Thông tin và Truyền thông đề nghị lãnh đạo các cơ quan, đơn vị chỉ đạo thực hiện một số biện pháp sau để hạn chế các rủi ro về nguy cơ mất an toàn thông tin, cụ thể:

1. Kiểm tra, rà soát các hệ thống thông tin đang sử dụng thiết bị mạng CISCO có khả năng bị ảnh hưởng bởi chiến dịch tấn công mạng ArcaneDoor. 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.

3. Khi phát hiện các hệ thống có biểu hiện bị khai thác, tấn công mạng, triển khai ngay các biện pháp xử lý ngăn chặn tấn công trên hệ thống và thông báo về Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi để có các biện pháp hỗ trợ, xử lý kịp thời.

(Gửi kèm Phụ lục thông tin về chiến dịch tấn công)

Đề nghị lãnh đạo các cơ quan, đơn vị quan tâm chỉ đạo thực hiện./.

Nơi nhận:

- Như trên;
- UBND tỉnh (báo cáo);
- Cục An toàn thông tin (báo cáo);
- Phòng VH&TT các huyện, thị xã, thành phố;
- Thành viên Đội ứng cứu sự cố ATTT mạng tỉnh;
- Sở TT&TT: Lãnh đạo Sở, các phòng chuyên môn, TT CNTT&TT;
- Lưu: VT, BCVT&CNTT.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Nguyễn Quốc Huy Hoàng

PHỤ LỤC
THÔNG TIN VỀ CHIẾN DỊCH TẤN CÔNG
(Kèm theo Công văn số /STTTT-BCVT&CNTT
ngày /5/2024 của Sở Thông tin và Truyền thông)

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/>
