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

Số: 152 /TTCNTT&TT-QTHT
V/v cảnh báo các lỗ hổng bảo mật nghiêm trọng và chiến dịch tấn công mạng bằng mã độc biến thể mới vào các hệ thống thông tin của các cơ quan, đơn vị

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

Thanh Hoá, ngày 09 tháng 5 năm 2024

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 tổ chức đoàn thể chính trị cấp tỉnh;
- Các doanh nghiệp VT, CNTT trên địa bàn tỉnh.

Căn cứ các Công văn cảnh báo an toàn thông tin của Cục An toàn thông tin, Bộ Thông tin và Truyền thông về việc xuất hiện các lỗ hổng bảo mật ảnh hưởng nghiêm trọng trên các phần mềm, ứng dụng. Đặc biệt, qua công tác giám sát an toàn thông tin mạng, ghi nhận các chiến dịch tấn công nhằm vào các thiết bị mạng Cisco có mức độ nghiêm trọng ảnh hưởng tới các hệ thống thông tin và nguy cơ mất an toàn thông tin. Cụ thể như sau:

- Lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong phần mềm PAN-OS

PAN-OS là một hệ điều hành tường lửa được triển khai dưới dạng tích hợp trên thiết bị phần cứng chuyên dụng hoặc ứng dụng độc lập. Trong thời gian qua, ghi nhận mã khai thác của lỗ hổng tồn tại trong phần mềm PAN-OS đã được sử dụng để tấn công vào hệ thống thông tin của nhiều cơ quan, tổ chức.

Lỗ hổng được gán nhãn theo chuẩn quốc tế có mã CVE-2024-3400 ảnh hưởng trên phần mềm PAN-OS. Thông tin về lỗ hổng này đặt ra một cảnh báo trong việc cần rà soát và nâng cấp phiên bản hoặc áp dụng biện pháp khắc phục thay thế cần được thực hiện ngay lập tức nếu tại các cơ quan, tổ chức có triển khai phần mềm này.

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

- Lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 04/2024

Ngày 09/04/2024, hãng Microsoft đã phát hành danh sách bản vá bảo mật định kỳ tháng 4/2024 với 147 lỗ hổng an toàn thông tin trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý vào các lỗ hổng an toàn thông tin có mức ảnh hưởng cao và nghiêm trọng sau:

+ Lỗ hổng an toàn thông tin **CVE-2024-20678** trong Remote Procedure Call Runtime (RPC) cho phép đối tượng tấn công thực thi mã từ xa.

+ Lỗ hổng an toàn thông tin **CVE-2024-29988** trong SmartScreen cho phép đối tượng tấn công vượt qua cơ chế bảo vệ.

+ **03** lỗ hổng an toàn thông tin **CVE-2024-21322, CVE-2024-21323, CVE-2024-29053** trong Microsoft Defender for IoT cho phép đối tượng tấn công thực thi mã từ xa.

+ Lỗ hổng an toàn thông tin **CVE-2024-20670** trong Outlook for Windows làm lộ lọt NTML hash, cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing).

+ Lỗ hổng an toàn thông tin **CVE-2024-26256** trong thư viện nguồn mở libarchive cho phép đối tượng tấn công thực thi mã từ xa.

+ Lỗ hổng an toàn thông tin **CVE-2024-26257** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

+ **07** lỗ hổng an toàn thông tin **CVE-2024-26221, CVE-2024-26222, CVE-2024-26223, CVE-2024-26224, CVE-2024-26227, CVE-2024-26231, CVE-2024-26233** trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa.

+ Lỗ hổng an toàn thông tin **CVE-2024-26234** trong Proxy Driver cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing).

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

- Phát hiện mã độc trojan Redline Stealer

Mã độc Trojan Redline Stealer hiện đang được sử dụng để tấn công vào hệ thống thông tin của nhiều cơ quan, tổ chức. Trong đó, ghi nhận một biến thể mới của mã độc trojan Redline Stealer đã được phát hiện trên không gian mạng, mã độc này được thiết kế dành riêng để thực hiện các hành vi độc hại. Số liệu thống kê cho thấy mã độc đang rất phổ biến trên toàn thế giới khi nó lây nhiễm và tấn công. Để

đảm bảo an toàn cho hệ thống thông tin, các cơ quan, tổ chức cần thực hiện kiểm tra, rà soát và chuẩn bị các phương án xử lý kịp thời khi phát hiện có dấu hiệu bị tấn công.

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

- Chiến dịch tấn công mới nhằm vào các thiết bị mạng Cisco

Qua công tác giám sát an toàn không gian mạng quốc gia, 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 có tại Phụ IV lục kèm theo)

Để bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin trong các cơ quan nhà nước trên địa bàn tỉnh, Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa đề nghị các cơ quan, đơn vị chỉ đạo các bộ phận, cá nhân thực hiện những nội dung sau:

1. Tổ chức kiểm tra, rà soát và xác định các máy tính trong phạm vi cơ quan, các đơn vị trực thuộc và UBND cấp xã đang sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng *(nếu có)* để kịp thời thực hiện cập nhật bản vá bảo mật nhằm hạn chế các nguy cơ bị tấn công, trong đó có mã độc trojan Redline Stealer; Đối với các phần mềm PAN-OS (*nếu có*) đang sử dụng có khả năng bị ảnh hưởng bởi lỗ hổng cần khẩn trương đánh giá và thực hiện nâng cấp lên phiên bản mới nhất (*Hướng dẫn chi tiết tại địa chỉ: https://attt.thanhhoa.gov.vn*).

2. Các cơ quan, đơn vị đang ghi nhận có kết nối mã độc và chưa cập nhật đầy đủ các lỗ hổng bảo mật trên các máy tính đã khuyến nghị (*chi tiết tại Phụ lục V kèm theo*). Đề nghị khẩn trương tiến hành kiểm tra, rà soát và khoanh vùng tìm kiếm để gỡ bỏ mã độc đang lây nhiễm trên các máy tính trong hệ thống mạng của đơn vị. Sau khi tiến hành thực hiện khắc phục xong, đề nghị các cơ quan, đơn vị thông báo kết quả xử lý về Trung tâm để tổng hợp, theo dõi.

3. Chỉ đạo Tổ ứng cứu sự cố an toàn thông tin mạng tại cơ quan, địa phương mình triển khai chủ động rà soát và sẵn sàng phương án xử lý sự cố khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời phổ biến, tuyên truyền kịp thời các nguy cơ về mất an toàn thông tin được cảnh báo của các cơ quan chức năng trong

phạm vi cơ quan, địa phương.

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 để phối hợp hỗ trợ, xử lý.

Điện thoại: (0237)3718.699; Thư điện tử: ungcuusuco@thanhhoa.gov.vn./.

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

Trần Ngọc Hưng

Phụ lục I
THÔNG TIN VỀ CÁC LỖ HỔNG AN TOÀN THÔNG TIN

1. Thông tin các lỗ hổng bảo mật

Mô tả: Lỗ hổng CVE-2024-3400 (Điểm CVSS: 10) ảnh hưởng trên phần mềm PAN-OS trong gateway GlobalProtect hiện đang bị sử dụng để khai thác. Đối tượng tấn công khai thác lỗ hổng chèn lệnh này có thể thực thi mã từ xa với quyền root trên tường lửa. Lỗ hổng gây ảnh hưởng cho tường lửa cấu hình trên GlobalProtect gateway và telemetry của thiết bị.

Lỗ hổng này ảnh hưởng đến các phiên bản:

- PAN-OS 11.1 trước bản 11.1.2-h3
- PAN-OS 11.0 trước bản 11.0.4-g1
- PAN-OS 10.2 trước bản 10.2.9-h1

- Bản vá cho các phiên bản bị ảnh hưởng sẽ được phát hành ngày 14/04/2024, người dùng nên cập nhật ngay khi khả dụng.

Dưới đây là một số IoC được ghi nhận:

- Update.py
- 3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac
- 5460b51da26c060727d128f3b3d6415d1a4c25af6a29fef4cc6b867ad3659078
- 172.233.228[.]93
- hxxp://172.233.228[.]93/policy
- hxxp://172.233.228[.]93/patch
- 66.235.168[.]222

2. Hướng dẫn khắc phục

Trước mắt, người dùng nên bật Threat ID 95187 và đảm bảo các biện pháp bảo mật lỗ hổng đã được áp dụng cho GlobalProtect. Trong trường hợp không thể bật Threat ID 95187, người dùng nên tạm thời tắt chức năng telemetry trên thiết bị cho tới cập nhật bản vá và chỉ nên bật lại sau khi đã cập nhật bản vá. Các bước để thực hiện việc tắt telemetry như sau:

1. Device > Setup >Telemetry;
2. Chọn widget Telemetry;
3. Bỏ chọn mục “Enable Telemetry”;
4. Bấm OK để lưu thay đổi.

3. Tài liệu tham khảo

https://security.paloaltonetworks.com/CVE-2024-3400
https://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-040

Phụ lục II
THÔNG TIN CÁC LỖ HỔNG BẢO MẬT THÁNG 04/2024

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-20678	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Remote Procedure Call Runtime (RPC) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20678
2	CVE-2024-29988	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong SmartScreen cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29988
3	CVE-2024-21322 CVE-2024-21323 CVE-2024-29053	- Điểm: CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21322

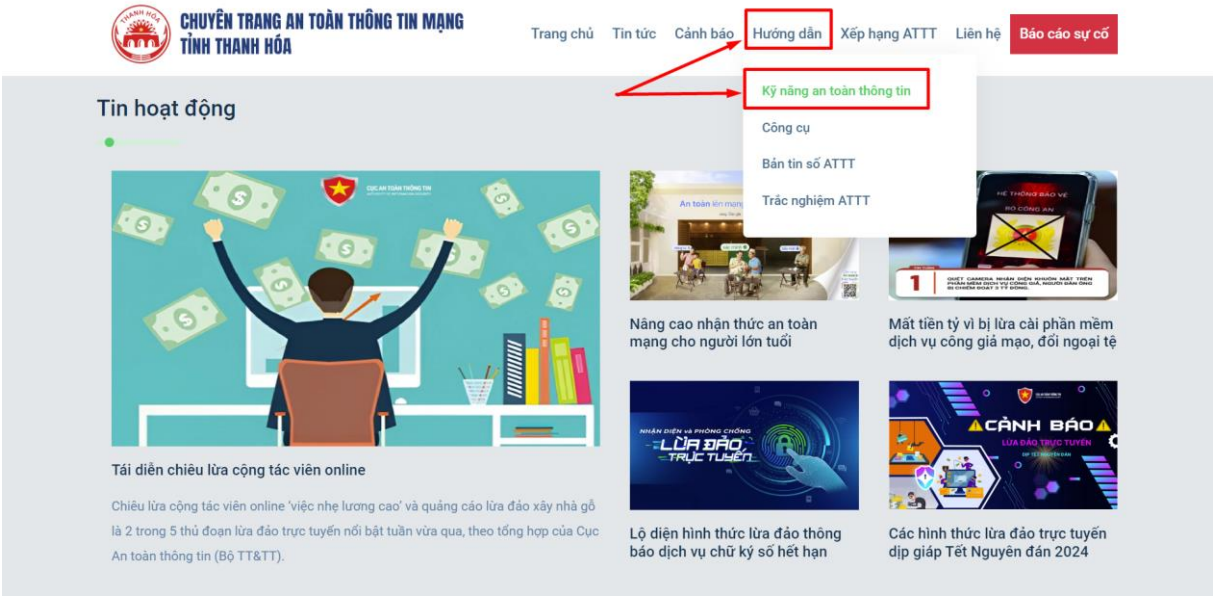
		Microsoft Defender for IoT cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Defender for IoT.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21323 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29053
4	CVE-2024-20670	- Điểm: CVSS: 8.1 (Cao) - Mô tả: Lỗ hổng trong Outlook for Windows làm lộ lọt NTML hash, cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). - Ảnh hưởng: Outlook for Windows.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20670
5	CVE-2024-26256	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong thư viện nguồn mở libarchive cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 11; Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26256
6	CVE-2024-26257	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26257

		xa. - Ảnh hưởng: Microsoft 365 Apps for Enterprise, Microsoft Office LTSC for Mac.	
7	CVE-2024-26221 CVE-2024-26222 CVE-2024-26223 CVE-2024-26224 CVE-2024-26227 CVE-2024-26231 CVE-2024-26233	- Điểm: CVSS: 7.2 (Cao) - Mô tả: Lỗ hổng trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26221 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26222 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26223 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26224 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26227 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26231 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26233
8	CVE-2024-26234	- Điểm: CVSS: 6.7 (Cao) - Mô tả: Lỗ hổng trong Proxy Driver cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). - Ảnh hưởng:	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26234

		Windows 10, Windows 11; Windows Server 2008, 2012, 2016, 2019, 2022.	

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng an toàn thông tin nói trên theo hướng dẫn của hãng. 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*). Các đơn vị tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại link nguồn tham khảo tại mục 1 của Phụ lục.



3. Tài liệu tham khảo

https://msrc.microsoft.com/update-guide/

https://www.zerodayinitiative.com/blog/2024/4/9/the-april-2024-security-updates-review

Phụ lục III
THÔNG TIN CHI TIẾT VỀ MÃ ĐỘC

1. Thông tin chi tiết về mã độc trojan Redline Stealer

RedLine Stealer là mã độc xuất hiện lần đầu tiên vào khoảng tháng 3 năm 2020, mã độc này có khả năng trích xuất thông tin đăng nhập từ nhiều nguồn khác nhau, bao gồm trình duyệt web, ứng dụng FTP, email, Steam, ứng dụng nhắn tin và VPN.

Một biến thể mới của mã độc trojan Redline Stealer đã được phát hiện trên không gian mạng, mã độc này triển khai các bytecode Lua để thực hiện các hành vi độc hại. Dữ liệu cho thấy mã độc đang rất phổ biến khi nó lây nhiễm trải dài Bắc Mỹ, Nam Mỹ, Châu Âu, Châu Á và Úc.

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

Dưới đây là một số IoC được ghi nhận

Cheat.Lab.2.7.2.zip	5e37b3289054d5e774c02a6ec491 5a60156d715f3a02aaceb7256cc3e bdc6610
Cheat.Lab.2.7.2.zip	https[:]//github[.]com/microsoft/vcpkg/files/1412 5503/Cheat.Lab.2.7.2.zip
lua51.dll	873aa2e88dbc2efa089e6efd1c8a5370e04c9f5749 d7631f2912bcb640439997
readme.txt	751f97824cd211ae710655e60a26885cd79974f0f 0a5e4e582e3b635492b4cad
compiler.exe	dfbf23697cfd9d35f263af7a455351480920a95bfc 642f3254ee8452ce20655a
Redline C2	213[.]248[.]43[.]58
Trojanised Git Repo	hxxps://github.com/microsoft/STL/files/1443256 5/Cheater.Pro.1.6.0.zip

2. Tài liệu tham khảo

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/redline-stealer-a-novel-approach/

Phụ lục IV
THÔNG TIN CHI TIẾT CHIẾN DỊCH TẤN CÔNG

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. Hướng dẫn khắc phục

- 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/

Phụ lục V

THÔNG TIN CÁC ĐƠN VỊ CÓ KẾT NỐI MÃ ĐỘC

STT	Đơn vị bị nhiễm	Địa chỉ kết nối mã độc
1	Sở Nông nghiệp và Phát triển Nông thôn	35.247.124.134
		34.101.226.87
2	Sở Văn hóa, Thể thao và Du lịch	34.91.94.238
3	UBND huyện Bá Thước	184.105.192.2
4	UBND huyện Nông Cống	34.91.94.238
		35.247.124.134