BẢN TIN NỘI BỘ
CẬP NHẬT VỀ AN TOÀN THÔNG TIN VÀ CẢNH BÁO LỖ HỔNG BẢO MẬT

1. Quy trình cung cấp, chuyển giao tài liệu, vật chứa bí mật nhà nước

Cung cấp, chuyển giao bí mật nhà nước cho cơ quan, tổ chức, người Việt Nam được giao thực hiện nhiệm vụ liên quan trực tiếp đến bí mật nhà nước

Theo Luật Bảo vệ bí mật nhà nước, người có thẩm quyền cho phép sao, chụp tài liệu, vật chứa bí mật nhà nước sẽ có quyền quyết định việc cung cấp, chuyển giao bí mật nhà nước. Bộ trưởng Bộ Quốc phòng, Bộ trưởng Bộ Công an quy định thẩm quyền cung cấp, chuyển giao bí mật nhà nước thuộc phạm vi quản lý.

Cơ quan, tổ chức và người Việt Nam được giao thực hiện nhiệm vụ liên quan trực tiếp đến bí mật nhà nước được đề nghị cung cấp, chuyển giao bí mật nhà nước.

Cơ quan, tổ chức đề nghị cung cấp, chuyển giao bí mật nhà nước phải có văn bản gửi người có thẩm quyền quyết định việc cung cấp, chuyển giao bí mật nhà nước. Văn bản đề nghị phải ghi rõ tên cơ quan, tổ chức; người đại diện cơ quan, tổ chức; bí mật nhà nước đề nghị cung cấp, chuyển giao; mục đích sử dụng và cam kết bảo vệ bí mật nhà nước.

Người đề nghị cung cấp, chuyển giao bí mật nhà nước phải có văn bản gửi người có thẩm quyền quyết định việc cung cấp, chuyển giao bí mật nhà nước. Văn bản đề nghị phải ghi rõ họ và tên; số Căn cước công dân, Chứng minh nhân dân, Hộ chiếu, Chứng minh Công an nhân dân hoặc số giấy chứng minh do Quân đội nhân dân cấp; địa chỉ liên lạc; vị trí công tác; bí mật nhà nước đề nghị cung cấp, chuyển giao; mục đích sử dụng và cam kết bảo vệ bí mật nhà nước.

Cung cấp, chuyển giao bí mật nhà nước cho cơ quan, tổ chức, cá nhân nước ngoài

Thẩm quyền quyết định việc cung cấp, chuyển giao bí mật nhà nước cho cơ quan, tổ chức, cá nhân nước ngoài được quy định như sau:

- Thủ tướng Chính phủ quyết định cung cấp, chuyển giao bí mật nhà nước độ Tuyệt mật;

- Bộ trưởng Bộ Quốc phòng, Bộ trưởng Bộ Công an, người có thẩm quyền (quy định tại khoản 1 điều 11) quyết định cung cấp, chuyển giao bí mật nhà nước độ Tối mật, độ Mật thuộc phạm vi quản lý.

Bí mật nhà nước chỉ được cung cấp, chuyển giao cho cơ quan, tổ chức, cá nhân nước ngoài tham gia vào chương trình hợp tác quốc tế hoặc thi hành công vụ có liên quan đến bí mật nhà nước.

Cơ quan, tổ chức nước ngoài đề nghị cung cấp, chuyển giao bí mật nhà nước phải có văn bản gửi cơ quan, tổ chức Việt Nam chủ trì chương trình hợp tác quốc tế hoặc thi hành công vụ có liên quan đến bí mật nhà nước. Văn bản đề nghị phải ghi rõ tên cơ quan, tổ chức, người đại diện cơ quan, tổ chức; quốc tịch, số Hộ chiếu, chức vụ của người đại diện; bí mật nhà nước đề nghị cung cấp, chuyển giao; mục đích sử dụng, cam kết bảo vệ bí mật nhà nước và không cung cấp, chuyển giao cho bên thứ ba nếu không có sự đồng ý của bên cung cấp, chuyển giao.

Cá nhân nước ngoài đề nghị cung cấp, chuyển giao bí mật nhà nước phải có văn bản gửi cơ quan, tổ chức Việt Nam chủ trì chương trình hợp tác quốc tế hoặc thi hành công vụ có liên quan đến bí mật nhà nước. Văn bản đề nghị phải ghi rõ họ và tên; số Hộ chiếu, địa chỉ liên lạc; bí mật nhà nước đề nghị cung cấp, chuyển giao; mục đích sử dụng, cam kết bảo vệ bí mật nhà nước và không cung cấp, chuyển giao cho bên thứ ba nếu không có sự đồng ý của bên cung cấp, chuyển giao.

Cơ quan, tổ chức Việt Nam chủ trì chương trình hợp tác quốc tế hoặc thi hành công vụ có liên quan đến bí mật nhà nước có trách nhiệm chuyển đề nghị của cơ quan, tổ chức, cá nhân nước ngoài đến người có thẩm quyền quyết định việc cung cấp, chuyển giao bí mật nhà nước.

Trường hợp từ chối cung cấp, chuyển giao bí mật nhà nước, người có thẩm quyền quyết định việc cung cấp, chuyển giao bí mật nhà nước phải trả lời bằng văn bản và nêu rõ lý do.

Link tham khảo: http://antoanthongtin.vn/chinh-sach---chien-luoc/quy-trinh-cung-cap-chuyen-giao-tai-lieu-vat-chua-bi-mat-nha-nuoc-106034

2. Máy tính có cổng Thunderbolt có thể bị đánh cắp dữ liệu thông qua 7 lỗ hổng mới

Mới đây một nhà nghiên cứu an ninh đã phát hiện ra 7 lỗ hổng phần cứng mới được cho là không thể khắc phục. Những lỗ hổng này ảnh hưởng đến tất cả các máy tính để bàn và laptop có cổng USB-C tương thích Thunderbolt hoặc cổng Thunderbolt.

ThunderSpy là cái tên được sử dụng để chỉ chung các lỗ hổng có thể bị khai thác bằng nhiều phương thức evil-maid khác nhau. Chúng chủ yếu được dùng để đánh cắp dữ liệu hoặc đọc/ghi tất cả bộ nhớ hệ thống của máy tính khi máy bị khóa hay khi máy trong trạng thái ngủ và rồi tấn công hệ thống.

Tóm lại, chỉ vài phút truy cập vật lý vào máy tính cũng có thể tạo ra cuộc tấn công evil-maid và gây hại cho người dùng.

Theo nhà nghiên cứu Björn Ruytenberg đến từ Đại học Công nghệ Eindhoven, cuộc tấn công ThunderSpy "có thể cần phải mở khung laptop bằng tuốc-nơ-vít, nhưng quan trọng là nó không để lại dấu vết xâm nhập và có thể thực hiện chỉ trong vài phút".

Nói cách khác, các lỗ hổng không được liên kết với đường link hay thành phần tương tự nào. Vì thế, nó không thể bị khai thác từ xa.

Ruytenberg cũng cho biết "Thunderspy hoạt động ngay cả khi bạn sử dụng nhiều cách bảo mật khác nhau. Ngay cả khi bạn khóa hoặc tạm dừng máy tính để đi ra ngoài trong khoảng thời gian ngắn, hoặc thậm chí quản trị hệ thống cài đặt Secure Boot, BIOS và mật khẩu tài khoản hệ điều hành mạnh, hay kích hoạt mã hóa toàn bộ ổ đĩa (full disk encryption) thì Thunderspy vẫn có thể hoạt động được".

Bên cạnh các máy tính chạy Windows hoặc Linux, một số máy tính Apple có cổng Thunderbolt được bán từ năm 2011 trở đi cũng trở thành nạn nhân của lỗ hổng này, trừ các phiên bản retina.

Dưới đây là danh sách về bảy lỗ hổng Thunderspy ảnh hưởng đến các phiên bản Thunderbolt 1, 2 và 3. Những lỗi này có thể bị khai thác để tạo bảng tính trạng thiết bị Thunderbolt tùy ý, sao chép các thiết bị Thunderbolt do người dùng ủy quyền và cuối cùng, có được kết nối PCIe (một dạng giao diện bus hệ thống/card mở rộng) để thực hiện các cuộc tấn công DMA (tấn công bảo mật bên trong).

- Schemes xác minh firmware không đầy đủ (Inadequate firmware verification schemes)
- Schemes xác thực thiết bị yếu (Weak device authentication schemes)
- Sử dụng siêu dữ liệu của thiết bị chưa được xác thực (Use of unauthenticated device metadata)
- Tấn công hạ cấp bằng cách sử dụng backward compatibility (Downgrade attack using backward compatibility)
- Sử dụng các cấu hình bộ điều khiển chưa được xác thực (Use of unauthenticated controller configurations)
- Thiếu sót giao diện flash SPI (SPI flash interface deficiencies)
- Không có bảo mật Thunderbolt trên Boot Camp (No Thunderbolt security on Boot Camp)

Các cuộc tấn công truy cập bộ nhớ trực tiếp (DMA) vào cổng Thunderbolt không phải là mới xuất hiện. Trước đây chúng đã được biết đến qua các cuộc tấn công ThunderClap.

Các cuộc tấn công DMA cho phép kẻ tấn công xâm nhập mục tiêu chỉ trong vài giây chỉ bằng cách cắm một thiết bị hot-plug độc hại như thẻ mạng ngoài, chuột, bàn phím, máy in hoặc thiết bị lưu trữ vào cổng Thunderbolt hoặc cổng USB-C.

Nói tóm lại, các cuộc tấn công DMA có thể xảy ra do cổng Thunderbolt hoạt động ở mức rất thấp và có quyền truy cập đặc quyền cao vào máy tính, cho phép các thiết bị ngoại vi được kết nối mà không cần thông qua các chính sách bảo mật của hệ điều hành và đọc/ghi trực tiếp vào bộ nhớ hệ thống. Trong bộ nhớ có thể chứa thông tin như mật khẩu, thông tin đăng nhập ngân hàng, các tập tin riêng tư và nhật ký hoạt động của trình duyệt.

Để ngăn chặn các cuộc tấn công DMA, Intel đã giới thiệu một số biện pháp đối phó. Một trong số đó là ‘security levels’, giúp ngăn các thiết bị có Thunderbolt PCIe kết nối trái phép mà chưa được sự cho phép của người dùng.

Nhà nghiên cứu cho biết “Để tăng khả năng xác thực thiết bị, hệ thống sẽ cung cấp ‘mật mã xác thực các kết nối’ nhằm ngăn chặn các thiết bị giả mạo việc được người dùng ủy quyền”.

Tuy nhiên, khi kết hợp ba lỗ hổng Thunderspy đầu tiên, kẻ tấn công có thể phá vỡ tính năng ‘security levels’ và bằng cách nạp một thiết bị Thunderbolt độc hại trái phép mạo danh thiết bị Thunderbolt đã được xác định.

Ruytenberg nói thêm “Bộ điều khiển Thunderbolt lưu trữ siêu dữ liệu của thiết bị trong firmware được gọi là Device ROM (DROM). Chúng tôi đã nhận thấy DROM

không được xác minh bằng mật mã.Từ đó, lỗ hổng này cho phép xây dựng các bộ giả mạo thiết bị Thunderbolt đã xác thực".

"Khi kết hợp với lỗ hổng thứ hai, những bộ xác nhận giả mạo có thể bao gồm một phần hoặc toàn bộ dữ liệu tùy ý"

"Ngoài ra, chúng tôi còn hiển thị các cấu hình Security Level không được xác thực như khả năng vô hiệu hóa hoàn toàn bảo mật Thunderbolt và khôi phục kết nối Thunderbolt nếu hệ thống bị hạn chế chỉ chuyển dữ liệu qua cổng USB và DisplayPort"

"Chúng tôi kết thúc báo cáo bằng việc chứng minh khả năng vô hiệu hóa vĩnh viễn bảo mật Thunderbolt và chặn tất cả các bản cập nhật firmware trong tương lai"

Theo Ruytenberg, một số hệ thống mới kể từ năm 2019 trong đó có tính năng bảo vệ Kernel DMA giúp giảm thiểu một phần các lỗ hổng Thunderspy.

Nhằm giúp mọi người kiểm tra thiết bị có bị ảnh hưởng bởi các lỗ hổng Thunderspy hay không, Ruytenberg cũng đã phát hành một công cụ mã nguồn mở miễn phí tên là Spycheck.

Trước khi được báo cáo lỗ hổng Thunderspy, Intel đã biết về một số lỗi nhưng lại không có kế hoạch vá lỗi hay tiết lộ cho công chúng.

Ruytenberg tuyên bố đã tìm thấy nhiều lỗ hổng tiềm năng trong giao thức Thunderbolt. Chúng hiện đang là một phần của dự án nghiên cứu đang diễn ra và dự kiến sẽ được tiết lộ ngay với tên gọi Thunderspy 2.

Nếu nghĩ đang sở hữu thiết bị có cổng Thunderbolt và nghĩ rằng mình là mục tiêu tiềm năng thì bạn hãy tránh để các thiết bị ở nơi không có người bảo vệ, tắt nguồn hoàn toàn hoặc ít nhất sử dụng chế độ ngủ đông thay vì chế độ ngủ.

Nếu rất lo sợ việc bị tấn công, hãy tránh để các thiết bị Thunderbolt ở nơi không giám sát được hoặc tránh cho người lạ mượn máy.

Khuyến nghị: Người dùng cần tuân thủ quy định tạo phân vùng riêng có mật khẩu để lưu trữ các dữ liệu nhạy cảm, tránh cho người lạ mượn máy tính để bảo đảm an toàn thông tin.

Link tham khảo: https://securitydaily.net/may-tinh-co-cong-thunderbolt-co-the-bi-danh-cap-du-lieu-thong-qua-7-lo-hong-moi/

3. Sử dụng Tivi để nghe lén thông tin vệ tinh nhạy cảm

Tin tặc đã sử dụng một loại thiết bị truyền hình tại nhà có giá khoảng 7 triệu đồng (300 đô la) để nghe lén các thông tin truyền thông vệ tinh nhạy cảm.

James Pavur, nhà nghiên cứu bảo mật của trường Đại học Oxford, vừa bắt được hàng terabyte dữ liệu từ lưu lượng vệ tinh trong thế giới thực, trong đó bao gồm thông tin nhạy cảm từ một số tổ chức lớn nhất thế giới.

Thông tin về cách thức tấn công mới này xuất hiện trong bối cảnh sẽ có sự thay đổi lớn về số lượng các vệ tinh trên quỹ đạo, từ khoảng 2.000 tại thời điểm hiện tại đến trên 15.000 vào năm 2030.

Dù chưa công bố chi tiết kỹ thuật tấn công nhưng Pavur cũng hé lộ một một vài thông tin.

Theo chuyên gia này, trong những điều kiện phù hợp, kẻ tấn công có thể dễ dàng hack được các cuộc họp đang diễn ra bằng các phương tiện liên kết vệ tinh.

Có vẻ như đó là do thiếu việc mã hóa quá trình truyền dẫn trong cách thức truyền thông băng thông rộng qua vệ tinh.

Pavur cho biết: "Cách thức truyền dữ liệu qua vệ tinh được sử dụng trong khoảng không gian lớn và sẽ chịu ảnh hưởng bởi độ trễ do tốc độ ánh sáng và thất thoát gói tin, từ đó có thể làm suy yếu chức năng của mô hình mã hóa được thiết kế dành cho các môi trường trên mặt đất có độ tin cậy cao. Ngoài ra, bản thân các vệ tinh cũng bị giới hạn về khả năng tính toán, đồng thời bất kỳ thao tác mã hóa on-board nào cũng có nguy cơ đánh đổi với một chức năng nhiệm vụ khác.

Bên cạnh đó, để có thể nghe lén sẽ cần sử dụng một chảo thu vệ tinh màn hình phẳng 75cm và một đầu thu TBS-6983 DVB-S được cấu hình để nhận truyền dẫn băng tần Ku ở dải 10.700 MHz và 12.750 MHz.

Thậm chí, Pavur còn tập trung vào các giao thức vệ tinh truyền hình kỹ thuật số (DVB-S) và DVB-S rendition 2 truyền thông tin theo định dạng MPEG-TS.

Chi tiết về cách thức tấn công sẽ được nhà bảo mật Pavur trình bày tại Hội thảo Black Hat diễn ra vào tháng 8 năm nay.

Link tham khảo: https://whitehat.vn/threads/su-dung-tivi-de-nghe-len-thong-tin-ve-tinh-nhay-cam.13662/

TECHNICAL PAGES:

1. Chi tiết về thông tin một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam trong tuần, cụ thể như sau:

STT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	IBM	CVE-2020-4285 CVE-2020-4422 CVE-2020-4287 …	Nhóm 23 lỗ hổng trong các sản phẩm của IBM (Sterling B2B Integrator,…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá.
2	Google	CVE-2020-0221 CVE-2020-0103 CVE-2020-0102 …	Nhóm 22 lỗ hổng trong phần mềm của Google (Google Android–Android 8,9,10) cho phép đối tượng tấn công truy cập trái phép, leo thang đặc quyền, tấn công tràn bộ đệm, chèn và thực thi mã từ xa. 01 lỗ hổng có CVSS:10,0 (đặc biệt nghiêm trọng).	Đã có thông tin xác nhận và bản vá
3	Red-hat	CVE-2020-1746 CVE-2020-1718 CVE-2020-1724 …	Nhóm 11 lỗ hổng trong các sản phẩm của Red- hat (jboss_keycloak, Ansible Engine, OpenShift Container,…) cho phép đối tượng tấn công truy cập trái phép, thu thập thông tin, chèn và thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá
4	Apache	CVE-2018-1285 CVE-2019-17572 CVE-2020-1945 …	Nhóm 10 lỗ hổng trong một số thành phần Apache (Log4net, ActiveMQ,…) cho phép đối tượng tấn công tấn công giả mạo XSS, tấn công directory traversal, tấn công tràn bộ đệm.	Đã có thông tin xác nhận và bản vá
5	Linux	CVE-2020-12769 CVE-2020-12771 CVE-2020-12826 …	Nhóm 09 lỗ hổng trong hệ điều hành Linux (Linux kernel <=5.6.13) cho phép đối tượng tấn công thu thập thông tin, tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
6	Samsung	CVE-2020-12747 CVE-2020-12748	Nhóm 09 lỗ hổng trong các phần mềm trên mobile	Đã có thông tin

		CVE-2020-12750 …	SamSung (O(8.X), Q(10.0),…) cho phép đối tượng tấn công thu thập thông tin, tấn công làm tràn bộ đệm, chèn và thực thi mã tùy ý. 01 lỗ hổng có CVSS:10,0 (đặc biệt nghiêm trọng).	xác nhận và bản vá
7	Vmware	CVE-2020-5409 CVE-2020-5407 CVE-2020-5408	Nhóm 03 lỗ hổng trong phần mềm Vmware (Pivotal Concourse <6.0.0, …) cho phép đối tượng tấn công truy cập trái phép, tấn công giả mạo.	Đã có thông tin xác nhận và bản vá
8	Wordpress	CVE-2020-11530 CVE-2020-12832 CVE-2020-12742	Nhóm 03 lỗ hổng trong phần mềm Wordpress (Chop Slider 3, simple-file-list plugin, iubenda- cookie-law-solution plugin,…) cho phép đối tượng tấn công chèn và thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá

2. Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

STT	**Tên miền/IP**
1	mel.cloudcontentsmak.com
2	soplifan.ru
3	ttheworkedreqsuchsun.com
4	xjpakmdcfuqe.ru
5	soplifan.ru
6	morphed.ru
7	zoroasterplace.com
8	cityofangelsmagazine.com
9	ydbnsrt.me
10	tttta.sssaaaas.io

3. Các cán bộ kỹ thuật đầu mối về ATTT cần thực hiện:
   - Xử lý các lỗ hổng phát hiện tại bảng 1 (nếu có).
   - Chặn, xử lý các truy nhập tới các tên miền độc hại tại bảng 2.