BẢN TIN NỘI BỘ

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

1. Lỗ hổng Bluetooth nghiêm trọng khiến các thiết bị dễ bị tấn công

Theo Engadget, tổ chức giám sát các tiêu chuẩn của công nghệ Bluetooth, Bluetooth SIG, đã đưa ra một thông báo bảo mật cho cuộc tấn công mà các nhà nghiên cứu gọi là Key Negotiation of Bluetooth hoặc KNOB.

Nó cung cấp cho những kẻ xấu can thiệp vào quy trình ghép nối Bluetooth, cho phép chúng tạo khóa mã hóa của kết nối ngắn hơn so với dự kiến. Từ đó, kẻ tấn công dễ dàng xâm nhập vào kết nối và có thể theo dõi dữ liệu được chia sẻ giữa các thiết bị, như giữa điện thoại với loa hoặc điện thoại và điện thoại khác.

Việc những kẻ tấn công có thể khai thác lỗ hổng ngay cả đối với các thiết bị đã được ghép nối trước đó khiến nó thực sự tồi tệ. Theo bài báo mà các nhà nghiên cứu công bố, lỗ hổng này ảnh hưởng đến các thiết bị sử dụng kết nối Bluetooth BR/EDR (hoặc Bluetooth Classic). Cuộc tấn công sẽ chỉ hoạt động nếu cả hai thiết bị thiết lập kết nối có lỗ hổng. Đáng chú ý, tất cả chip Bluetooth mà các nhà nghiên cứu đã thử nghiệm đều dễ bị tấn công.

Báo cáo cho hay, cuộc tấn công KNOB có thể xảy ra do lỗi trong thông số kỹ thuật Bluetooth. Do đó, mọi thiết bị Bluetooth tuân thủ tiêu chuẩn đều có thể bị tổn thương, với dẫn chứng hơn 17 chip Bluetooth trên 24 thiết bị khác nhau đều bị tấn công. Các chip đều dễ bị tấn công bởi KNOB trải rộng từ các nhà sản xuất Broadcom, Qualcomm, Apple, Intel và Chicony.

Những gã khổng lồ công nghệ như Apple và Microsoft đã tung ra các bản vá để khắc phục lỗ hổng và Bluetooth Core Specification đã được thay đổi để yêu cầu độ dài khóa mã hóa tối thiểu. Những biện pháp này được đưa ra để chống lại những gì mà các nhà nghiên cứu gọi là "mối đe dọa nghiêm trọng đối với bảo mật và quyền riêng tư của tất cả người dùng Bluetooth".

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần cập nhật các bản vá mới nhất của thiết bị đang sử dụng để khắc phục lỗ hổng và đảm bảo an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/lo-hong-bluetooth-nghiem-trong-khien-cac-thiet-bi-de-bi-tan-cong-1115875.html

2. Microsoft công bố 4 lỗ hổng Remote Desktop mới ảnh hưởng nhiều phiên bản Windows

Microsoft vừa cho biết hệ điều hành Windows có chứa bốn lỗ hổng nghiêm trọng trong Dịch vụ Remote Desktop, tương tự như lỗ hổng RDP 'BlueKeep' được vá gần đây.

Được phát hiện bởi nhóm an ninh của Microsoft, cả bốn lỗ hổng, CVE-2019-1181, CVE-2019-1182, CVE-2019-1222 và CVE-2019-1226, đều có thể bị khai thác bởi những kẻ tấn công trái phép từ xa để chiếm quyền điều khiển hệ thống máy tính bị ảnh hưởng mà không yêu cầu bất kỳ tương tác người dùng.

Giống như lỗ hổng RDP BlueKeep, cả bốn lỗ hổng đều có thể bị phần mềm độc hại khai thác để tự động lan truyền từ một máy tính tồn tại lỗ hổng sang máy tính khác (wormable).

"Kẻ tấn công có thể thực thi mã ở cấp hệ thống bằng cách gửi gói RDP tự tạo đặc biệt tới máy chủ RDS bị ảnh hưởng", Microsoft cảnh báo.

"Các phiên bản Windows bị ảnh hưởng là Windows 7 SP1, Windows Server 2008 R2 SP1, Windows Server 2012, Windows 8.1, Windows Server 2012 R2 và tất cả các phiên bản Windows 10 được hỗ trợ, bao gồm cả phiên bản máy chủ".

Mặc dù hai lỗ hổng CVE-2019-1181 và CVE-2019-1182 ảnh hưởng đến tất cả các phiên bản được hỗ trợ của Windows, hai lỗ hổng CVE-2019-1222 và CVE-2019-1226 chỉ ảnh hưởng đến Windows 10 và Windows Server Editions.

Các lỗ hổng không ảnh hưởng đến Windows XP, Windows Server 2003 và Windows Server 2008 cũng như không ảnh hưởng đến chính Giao thức Remote Desktop (RDP) mà Microsoft đã phát triển cho Remote Desktop Services.

Thay vào đó, các lỗ hổng nằm trong Dịch vụ Remote Desktop, trước đây được gọi là Terminal Services, có thể bị khai thác bởi những kẻ tấn công trái phép từ xa bằng cách gửi các yêu cầu tự tạo đặc biệt qua giao thức RDP đến một hệ thống mục tiêu.

Microsoft cũng thông tin rằng không tìm thấy bất kỳ bằng chứng cho thấy những lỗ hổng này đã được bất kỳ bên thứ ba biết đến hay đang bị khai thác trong thực tế.

"Điều quan trọng là các hệ thống bị ảnh hưởng phải được vá càng sớm càng tốt vì các rủi ro liên quan đến các lỗ hổng như thế này", Microsoft khuyến cáo mạnh mẽ.

Nếu không được vá, các lỗ hổng này có thể cho phép kẻ tấn công phát tán phần mềm độc hại theo cách tương tự như WannaCry và NotPetya khét tiếng đã lan rộng trên toàn cầu vào năm 2017.

Bản cập nhật Patch Tuesday tháng 8 năm 2019

Bên cạnh bốn lỗi an ninh quan trọng này, trong bản cập nhật Patch Tuesday tháng 8, Microsoft cũng vá 89 lỗ hổng, 25 trong số đó được đánh giá là nghiêm trọng và 64 lỗi ở mức độ quan trọng.

Bản cập nhật Patch Tuesday tháng 8 năm 2019 bao gồm bản vá cho các phiên bản Windows được hỗ trợ khác nhau và các sản phẩm khác của Microsoft gồm Internet Explorer, Edge, Office, ChakraCore, Visual Studio, Online Services và Active Directory Microsoft Dynamics.

Tất cả các lỗ hổng nghiêm trọng được liệt kê trong tháng này đều ảnh hưởng đến các phiên bản khác nhau của Windows 10 và phiên bản Server và chủ yếu nằm trong Chakra Scripting Engine, một số nằm trong Windows Graphics Device Interface (GDI), Word, Outlook, Hyper-V và VBScript Engine, LNK và Windows DHCP Server.

Một số lỗ hổng được xếp hạng quan trọng cũng dẫn đến các cuộc tấn công thực thi mã từ xa, trong khi phần lớn lỗ hổng còn lại cho phép nâng cao đặc quyền, từ chối

dịch vụ, tiết lộ thông tin, vượt qua biện pháp bảo vệ, giả mạo và tấn công kịch bản chéo.

Người dùng và quản trị viên hệ thống được khuyến cáo cập nhật các bản vá an ninh mới nhất càng sớm càng tốt để ngăn chặn tội phạm mạng và tin tặc kiểm soát máy tính của họ.

Để cài đặt các bản cập nhật mới nhất, bạn có thể vào Settings → Update & Security → Windows Update → Check for updates trên máy tính của bạn hoặc bạn có thể cài đặt các bản cập nhật theo cách thủ công.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng và người quản trị cần cập nhật các bản vá mới nhất của hệ điều hành để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/microsoft-cong-bo-4-lo-hong-remote-desktop-moi-anh-huong-nhieu-phien-ban-windows.12574/

3. Hãi hùng với sạc iPhone giả mạo kiểu mới: Cắm vào là thoải mái hack, điều khiển máy nạn nhân từ xa

Cắm dây sạc iPhone vào iPhone rồi kết nối với máy tính, đó là chuyện quá đỗi quen thuộc đối với những ai dùng đồ Apple. Tải nhạc offline, nạp pin tạm khi không có củ sạc, kiểm tra thông tin máy... hàng ti tỉ thứ có thể làm nhờ sự kết hợp của 2 thiết bị. Chỉ cần một bước xác nhận trên iPhone rằng chủ nhân có chấp nhận cho phép kết nối hay không và XONG, tất cả hoàn thành chỉ trong một nốt nhạc.

Thế nhưng, thế giới ngày nay không đơn giản và dễ đoán đến vậy khi mới đây, một loại hình dây sạc giả đội lốt hàng thật đã được phát hiện. Thay vì chỉ cắm và làm mọi thứ như chúng ta nghĩ thông thường, sợi dây giả này có thể giúp hacker điều khiển thiết bị của nạn nhân từ xa nhờ những thành phần chủ ý được thêm vào bên trong sợi dây cáp.

"Trông nó y hệt như mọi chiếc dây sạc Apple khác, và cũng hoàn toàn tương thích khi kết nối với các thiết bị. Mọi thứ chỉ trở nên bất thường nếu chúng ta đủ trình độ phát hiện ra đó là đồ giả và có can thiệp để xâm nhập trái phép," một chuyên gia với bí danh MG chia sẻ với phóng viên Motherboard tại sự kiện an ninh công nghệ Def Con.

Một kế hoạch xấu xa có thể được lên phương án và thực hiện dễ dàng chỉ qua vài cử chỉ và hành động nhỏ, chẳng hạn như nhanh tay tráo dây sạc hoặc tặng bộ sạc này làm quà cho mục tiêu. Sẽ chẳng ai mảy may nghi ngờ gì vì kiến thức chuyên môn của họ chưa đủ nhạy bén tới mức đó.

Sau khi con mồi đã sập bẫy và sử dụng sợi dây này để kết nối với máy tính trong một khoảnh khắc nào đó, kẻ gian từ xa có thể xâm nhập và tiến hành một loạt hành động tùy ý thích. Đúng như cách mà MG thử nghiệm tại Def Con, anh ta cho thấy mình có thể truy cập dữ liệu thông qua địa chỉ kết nối của sợi dây, sau đó tự tay chạy hàng tá chương trình riêng của hacker. "Nó giúp tôi thao tác với máy tính của mục tiêu như thể tôi đang ngồi ngay tại bàn làm việc nơi đặt máy tính đó mà chủ nhân không hề hay biết vậy," MG chia sẻ.

Chưa hết, nếu phát hiện nguy cơ bị lần ra, kẻ gian có thể tự hủy chứng cớ bằng cách vô hiệu hóa thành phần và chức năng xâm nhập bên trong sợi dây. Các thành phần này thực ra là linh kiện cực nhỏ được lắp đặt thủ công, sau đó bọc lớp cao su ra ngoài cùng một cách tinh vi sao cho trông y hệt sản phẩm gốc của Apple. MG cũng tiết lộ không sớm thì muộn mình cũng làm được các sợi dây sạc tương tự nhưng làm giả được cả hàng thương hiệu khác.

200 USD là mức giá MG đặt cho một sợi dây sạc đặc biệt này, nhưng sẽ giới hạn người dùng dưới mục đích phục vụ nghiên cứu an ninh mạng chứ không dành cho mục đích xấu, khởi điểm là cho công ty Hak5 mà anh đang làm việc.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần sử dụng hàng chính hãng, không mua hàng không rõ nguồn gốc xuất xứ và đề cao cảnh giác để tránh nguy cơ mất an toàn thông tin.

Link tham khảo: http://ttvn.vn/cong-nghe/hai-hung-voi-sac-iphone-gia-mao-kieu-moi-cam-vao-la-thoai-mai-hack-dieu-khien-may-nan-nhan-tu-xa-212019128145514304.htm

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	Cpanel	CVE-2017-18386 CVE-2017-18460 CVE-2017-18474 ...	Nhóm 117 lỗ hổng trên Cpanel cho phép đối tượng tấn công chèn và thực thi mã lệnh độc hại qua nhiều thành phần khác nhau (PostgreSQL, SQLite, /scripts/maildir_converter, BoxTrapper API...). Việt Nam có ít nhất 210 máy chủ Cpanel đang công khai trên Internet. Đã có cảnh báo 249 lỗ hổng của Cpanel trong tuần 31.	Đã có thông tin xác nhận và bản vá.
2	Magento	CVE-2019-7890 CVE-2019-7930 CVE-2019-7851 …..	Nhóm 71 lỗ hổng trên Magento (nền tảng nguồn mở hỗ trợ xây dựng website thương mại điện tử) cho phép truy cập trái phép vào hệ thống, khai thác lỗi file update để cài cắm mã độc trên hệ thống. Lỗ hổng CVE-2019-7930 có điểm CVSS là 9.0	Đã có thông tin xác nhận và bản vá.
3	OpenEMR	CVE-2019-14529	Lỗ hổng trên OpenEMR cho phép đối tượng tấn công khai thác lỗi SQL Injection thông qua /forms/eye_mag/save.php. OpenEMR là phần mềm quản lý hồ sơ sử dụng trong lĩnh vực y tế, nếu ứng dụng này bị khai thác thì có thể gây ra các vụ lộ lọt thông tin của bệnh nhân tại các bệnh viện.	Đã có phương án khắc phục
4	D-Link	CVE-2019-6968 CVE-2019-6969	Nhóm 02 lỗ hổng trên firmware của thiết bị D-Link DVA-5592 20180823 cho phép khai thác lỗi XSS, truy cập trái phép vào thiết bị để lấy thông tin như mật khẩu Wi-Fi, số điện thoại (nếu sử	Đã có thông tin xác nhận và bản vá

			dụng VoIP)	
5	Jira	CVE-2018-20826 CVE-2018-20827 CVE-2019-11581	Nhóm 03 lỗ hổng trên phần mềm quản lý dự án Jira cho phép đối tượng tấn công khai thác lỗi XSS, chèn và thực thi mã lệnh trên hệ thống. Có 22 máy chủ của Việt Nam đang public trên Internet có sử dụng Jira. Lỗ hổng CVE-2019-11581 đã được Cục ATTT cảnh báo trực tiếp đến 1 số đơn vị đang có máy chủ Jira bị ảnh hưởng từ 23/7/2019.	Đã có thông tin xác nhận và bản vá
6	Cisco	CVE-2019-1971 CVE-2019-1910 CVE-2019-1918 …	Nhóm 32 lỗ hổng trên một số sản phẩm ứng dụng của Cisco (NFVIS, IOS XR Software, Firepower Threat Defense software, IoT Field Network Director, Small Business 220 Series Smart Switches...) cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, khai thác lỗi XSS, CSRF, chèn và thực thi mã lệnh, tấn công leo thang	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	n.hmiblgoja.ru
2	mel.cloudcontentsmak.com
3	mokoaehaeihgiaheih.ru
4	realhotchickss.com
5	ajkeahkcueafuiaeuf.ru
6	pradanewstyle.com
7	bszotsjovih.com
8	strikotunrev.top
9	letstryitnowx.online
10	willem@alternativa.nl:444134

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.