BẢN TIN NỘI BỘ

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

1. Dell khuyến cáo người dùng PC cập nhật SupportAssist

Dell đã đưa ra một cảnh báo bảo mật cho khách hàng về việc cập nhật SupportAssist cho các máy PC, để khắc phục lỗ hổng bảo mật có tên Had Hadar. Lỗ hổng này được đánh giá mức độ nghiêm trọng và định danh CVE-2019-12280.

Theo thông báo trên trang web của Dell, SupportAssist được cài đặt mặc định trên hầu hết các thiết bị Dell chạy hệ điều hành Windows. Điều này có nghĩa, nếu phần mềm này không được cập nhật kịp thời, lỗ hổng Had Hadar sẽ ảnh hưởng đến hàng triệu người dùng máy tính Dell.

Lỗ hổng tồn tại trong SupportAssist được phát hiện bởi nhà nghiên cứu bảo mật SafeBreach Labs. Sau khi SafeBreach Labs gửi thông tin chi tiết về lỗ hổng cho Dell, thì các nhà nghiên cứu lại tiếp tục phát hiện ra rằng lỗ hổng này ảnh hưởng đến cả các OEM bổ sung sử dụng một phiên bản đổi thương hiệu (rebranded version) của PC-Doctor Toolbox cho các thành phần của phần mềm Windows.

Công ty sản xuất và duy trì công cụ sửa chữa phần mềm Pc-Doctor cho biết, công ty đã biết về lỗ hổng Had Hadar. Tuy nhiên, sẽ rất ít khả năng một người dùng có đủ quyền để khai thác lỗ hổng này.

Để khai thác, người dùng hoặc quy trình quản trị sẽ phải thay đổi biến môi trường PATH của hệ thống để bao gồm một thư mục có thể ghi bởi người dùng không phải quản trị viên và tạo một DLL khai thác các đặc quyền quản trị. Điều đó dẫn đến việc không thể khai thác lỗ hổng này mà không thay đổi cài đặt Windows mặc định.

Lỗ hổng trong SupportAssist được báo cáo lần đầu vào ngày 29/4/2019. Theo báo cáo ban đầu của Dell, lỗ hổng này được khai thác nhắm mục tiêu vào dịch vụ "Hỗ trợ phần cứng của Dell' với kịch bản: Kẻ tấn công sẽ khai thác dịch vụ để chiếm quyền truy cập vào phần cứng PC để thực hiện leo thang đặc quyền trong hệ thống. Khi đó, kẻ tấn công có thể tải và cài đặt các phần mềm độc hại vào thiết bị và che dấu chúng mà hoàn toàn không bị phát hiện. Lỗ hổng này ảnh hưởng đến Dell SupportAssist for Business PC phiên bản 2.0.1 và Dell SupportAssist cho Home PC phiên bản 3.2.2.

Vào ngày 28/5/2019, các bản sửa lỗi được cung cấp bởi PC-Doctor cho các phiên bản SupportAssist đã được Dell phát hành. Theo như khuyến cáo, thành phần PC Doctor trong Dell SupportAssist cho Business Systems và Dell SupportAssist cho Home PC đều đã được cập nhật.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng Dell cần cập nhật SupportAssist lên phiên bản mới nhất để đảm bảo an toàn thông tin.

Link tham khảo:

http://www.antoanthongtin.vn/Detail.aspx?NewsID=b2611d2b-b0eb-4956-adde-c0cccb181051&CatID=751fd4e7-4da5-4f31-85aa-be0240fe4910&MenuID=751fd4e7-4da5-4f31-85aa-be0240fe4910

2. 50 triệu người dùng bị ảnh hưởng vì lỗ hổng trên Windows 10

Theo nguồn tin từ Forbes, Microsoft đã đưa ra lời cảnh báo đến 10 triệu người dùng Windows 10 rằng bản cập nhật mới nhất mang tên KB4501375 có thể gây lỗi cho dịch vụ Trình quản lý kết nối truy cập từ xa (RASMAN). Điều này có thể sẽ gây ra những hậu quả nghiêm trọng cho máy tính người dùng.

Mạng riêng ảo hay còn gọi là VPN sẽ bị ảnh hưởng nhiều nhất vì lỗi này. Dịch vụ RASMAN quản lý các kết nối của Windows 10 đến hệ thống Internet và là nền tảng quan trọng để VPN có thể hoạt động.

Đội ngũ Windows sau đó đã tổng hợp các trường hợp gặp lỗi được ghi nhận. Cụ thể, dịch vụ RASMAN sẽ đột ngột ngừng hoạt động và quản trị viên hoặc người dùng trên hệ thống sẽ nhận được thông báo lỗi 0xc0000005.

Theo Globenewswire, nhu cầu sử dụng VPN hiện nay đang ngày càng tăng cao hơn. Với nhiều mục đích sử dụng khác nhau như truy cập nền tảng xem phim Netflix hay các trang web hạn chế quốc gia, VPN có tiềm năng để tác động mạnh mẽ vào máy tính cá nhân người dùng.

Microsoft cho biết các máy tính đang chạy trên nền tảng Windows 10 phiên bản 1903, đặc biệt là đã cài đặt bản cập nhật KB4497935 sẽ có nguy cơ cao gặp phải lỗi này. Vấn đề càng nghiêm trọng hơn khi số lượng người dùng bị ảnh hưởng đã lên tới con số hơn 50 triệu.

Trước đó, vào ngày 7/6, Microsoft và Cơ quan An ninh Quốc gia Mỹ (NSA) đã kêu gọi người dùng Windows cập nhật hệ điều hành sau khi phát hiện lỗ hổng nghiêm trọng BlueKeep.

Lỗ hổng được đánh giá nguy hiểm đến mức Microsoft phải ra bản cập nhật cho hệ điều hành bị "khai tử" từ năm 2014, Windows XP. NSA cho biết BlueKeep có thể lây lan trên Internet và tạo ra các cuộc tấn công nhằm mục đích tống tiền người dùng như mã độc WannaCry 2 năm trước.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng Windows 10 cần cập nhật hệ điều hành ngay khi có phiên bản mới để đảm bảo an toàn thông tin.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/50-trieu-nguoi-dung-bi-anh-huong-vi-lo-hong-tren-windows-10-548256.html

3. Phát hiện lỗ hổng bảo mật nghiêm trọng đe dọa người dùng Mac

Nhà nghiên cứu bảo mật Jonathan Leitschuh vừa tiết lộ lỗ hổng zero-day nghiêm trọng trong ứng dụng hội nghị truyền hình Zoom trên máy Mac.

Theo Theverge, Leitschuh đã chứng minh rằng bất kỳ trang web nào cũng có thể mở một cuộc gọi kích hoạt video trên máy Mac với ứng dụng Zoom được cài đặt. Đó là vì ứng dụng Zoom dường như cài đặt một máy chủ web trên Mac chấp nhận các yêu cầu trình duyệt thông thường. Trên thực tế, nếu người dùng gỡ cài đặt Zoom thì máy chủ web vẫn tồn tại và có thể cài đặt lại Zoom mà không cần sự can thiệp của người dùng.

Sử dụng bản demo của Leitschuh, TheVerge đã xác nhận rằng lỗ hổng này thực sự đang hoạt động. Khi nhấp vào một liên kết nếu trước đó bạn đã cài đặt ứng dụng Zoom, nó sẽ đưa người dùng tự động tham gia cuộc gọi hội nghị truyền hình với máy ảnh trên thiết bị.

Leitschuh cho biết đã tiết lộ lỗ hổng cho Zoom vào cuối tháng 3 và cho công ty 90 ngày để giải quyết vấn đề. Tuy nhiên, Zoom dường như đã không làm hết trách nhiệm của mình để xử lý lỗi này. Lỗ hổng cũng được tiết lộ cho cả hai nhóm Chromium và Mozilla, nhưng vì nó không xuất phát từ trình duyệt của họ nên mọi thứ không thể xử lý được.

Báo cáo cho biết sự tồn tại của máy chủ web trên máy tính Mac là một vấn đề vô cùng nghiêm trọng cho người sử dụng. Ví dụ, nó có thể mở ra một cuộc tấn công từ chối dịch vụ trên máy Mac bằng cách liên tục ping máy chủ web.

Cũng theo Leitschuh, mọi người có thể tự vá lỗi này bằng cách đảm bảo ứng dụng Zoom được cập nhật và vô hiệu hóa cài đặt cho phép Zoom bật máy ảnh khi tham gia cuộc họp. Lưu ý, gỡ cài đặt Zoom sẽ không chắc khắc phục được sự cố vì máy chủ web vẫn tồn tại trên máy Mac. Tắt máy chủ web yêu cầu chạy một số lệnh đầu cuối.

Hiện tại, Zoom cho biết máy chủ web là một giải pháp hợp pháp để đảm bảo trải nghiệm người dùng, cho phép họ có thể tham gia cuộc họp dễ dàng bằng thao tác nhấp chuột. Tuy nhiên, công ty cho biết sẽ bảo vệ người dùng trong bản vá lỗi tương lai, và những thay đổi sẽ được áp dụng trên tất cả nền tảng của họ. Bên cạnh đó, Zoom cũng loại bỏ khả năng tự động đưa người dùng tham gia cuộc gọi hội nghị truyền hình với máy ảnh trên thiết bị.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng MacOS cần đảm bảo ứng dụng Zoom được cập nhật và vô hiệu hóa cài đặt cho phép Zoom bật máy ảnh khi tham gia cuộc họp để đảm bảo an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/phat-hien-lo-hong-bao-mat-nghiem-trong-de-doa-nguoi-dung-mac-1101424.html

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	Cisco	CVE-2019-1922 CVE-2019-1932 CVE-2019-1889 CVE-2019-1933 ...	Nhóm 18 lỗ hổng trên một số sản phẩm của Cisco (Phần mềm điện thoại IP SIP, AsyncOS) cho phép kẻ tấn công thực hiện tấn công từ chối dịch vụ, chèn và thực thi mã lệnh, tấn công leo thang để chiếm quyền kiểm soát thiết bị.	Đã có thông tin xác nhận và bản vá
2	IBM	CVE-2019-4057 CVE-2019-4154 CVE-2019-4322 CVE-2019-4369 …..	Nhóm 26 lỗ hổng dựa trên một số sản phẩm của IBM (DB2, Security Guardium, WebSphere Application Server) cho phép kẻ tấn công xác thực cục bộ thực thi mã tùy ý trên hệ thống, gây tràn bộ đệm. Truy cập tài khoản DB2 thực mã tùy ý và lấy thông tin nhạy cảm.	Đã có thông tin xác nhận và bản vá
3	Wordpress	CVE-2019-5971 CVE-2019-5962 CVE-2019-12826 ……..	Nhóm 13 lỗ hổng trên máy chủ sử dụng Wordpress cho phép kẻ tấn công khia thác lỗi CSRF, XSS để lấy thông tin xác thực và chiếm quyền quản trị viên, thay đổi cài đặt ứng dụng.	Đã có thông tin xác nhận và bản vá.
4	Jetbrains	CVE-2019-12842 CVE-2019-12845 CVE-2019-12846 ……	Nhóm 21 lỗ hổng trên sản phẩm của Jetbrains (JetBrains Hub, IntelliJ IDEA, Ktor) cho phép người dùng tạo kết nối không được mã hóa làm lộ thông tin đăng nhập, một số lỗ hổng cho phép thực hiện tấn công từ xa thực thi mã khi cấu hình đang chạy.	Đã có thông tin xác nhận và bản vá.
5	D-Link	CVE-2019-13373 CVE-2019-13374	Nhóm 19 lỗ hổng trên một số sản phẩm của D-Link (Central	Đã có thông tin xác nhận

		CVE-2019-13375 …	WiFi Manager CWM, D-Link DCS-1100, DCS-1130) cho phép đối tượng khai thác lỗi SQL Injection qua nhiều tham số khác nhau, thực thi các đoạn mã PHP độc hại, khai thác lỗi tràn bộ đệm để cài cắm mã độc vào thiết bị.	và bản vá.

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

STT	**Tên miền/IP**
1	differentia.ru
2	disorderstatus.ru
3	atomictrivia.ru
4	soplifan.ru
5	somicrososoft.ru
6	www.cityofangelsmagazine.com
7	kodklq.info
8	morphed.ru
9	bharatisangli.in
10	www.corpnox-technologie.fr

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.