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

1. Windows 7 sẽ chính thức ngừng hoạt động

Từ ngày 14/01/2020, các máy tính cá nhân sử dụng hệ điều hành Windows 7 sẽ vẫn hoạt động, nhưng sẽ không còn được Microsoft hỗ trợ kỹ thuật, cập nhật phần mềm hoặc cập nhật bảo mật.

Microsoft cũng sẽ triển khai các thông báo trên toàn màn hình cho người dùng Windows 7 từ giữa tháng 01/2020, nhằm buộc người dùng nâng cấp lên Windows 10 hoặc từ bỏ hệ điều hành sắp bị ngừng hoạt động này.

Microsoft đã tạo các cửa sổ nhỏ trên máy tính người dùng nhắc về sự thay đổi sắp tới kể từ tháng 04/2019, nhưng sẽ thay thế các thông báo này bằng các cửa sổ thông báo trên toàn màn hình để khiến người dùng Windows 7 khó bỏ qua hơn.

Theo NetMarketShare, tính đến tháng 11/2019, hệ điều hành Windows 7 vẫn đang được sử dụng bởi 26,86% người dùng Windows. Trong khi đó, hệ điều hành hiện hành Windows 10 chiếm thị phần 53,33%.

Windows 7 là một hệ điều hành máy tính cá nhân được Microsoft sản xuất như là một phần của gia đình hệ điều hành Windows NT. Nó được phát hành để đưa vào các máy tính sản xuất vào ngày 22/7/2009 và có sẵn để người dùng tải về tự cài đặt vào ngày 22/10/2009, chưa đầy ba năm sau khi phiên bản tiền nhiệm Windows Vista phát hành.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người quản trị và người dùng nếu còn sử dụng Windows 7 cần cập nhật hệ điều hành lên Windows 10 để đảm bảo an toàn thông tin.

Link tham khảo: http://antoanthongtin.vn/tin-tuc-san-pham/windows-7-se-chinh-thuc-ngung-hoat-dong-105739

2. Nhiều thiết bị định tuyến D-Link bị ảnh hưởng bởi lỗ hổng thực thi lệnh từ xa

Đầu năm 2020, các nhà nghiên cứu an ninh mạng vừa công khai loạt mã khai thác PoC cho các lỗ hổng tiết lộ thông tin và thực thi lệnh từ xa ảnh hưởng đến rất nhiều thiết bị định tuyến D-link (D-Link router).

Hai nhà nghiên cứu, Miguel Méndez Zúñiga và Pablo Pollanco của Telefónica Chile, đã tiết lộ thông tin về các lỗ hổng. Ngoài các chi tiết kỹ thuật và mã PoC, còn có các video minh họa cách thức khai thác lỗ hổng.

D-Link đã biết về các lỗ hổng từ giữa tháng 10, tuy nhiên hãng chỉ liệt kê các bộ định tuyến DIR-859 trong danh sách bị ảnh hưởng.

Trên thực tế, các lỗ hổng thực sự ảnh hưởng đến hàng tá mô hình D-Link DIR, bao gồm cả những mô hình không còn được hỗ trợ.

Nhà cung cấp đã phát hành các bản cập nhật firmware giải quyết các lỗ hổng cho một số thiết bị bị ảnh hưởng và sẽ sớm phát hành các bản vá cho số thiết bị còn lại, bao gồm DIR-818Lx đã không còn được hỗ trợ. Các mô hình bị ảnh hưởng khác không còn được hỗ trợ sẽ không được vá.

Lỗ hổng thực thi lệnh từ xa, CVE-2019-17621, liên quan đến cách xử lý các yêu cầu UpnP, có thể cho phép kẻ tấn công không xác thực được quyền kiểm soát các thiết bị tồn tại lỗ hổng.

Tuy nhiên, việc khai thác đòi hỏi quyền truy cập vào mạng LAN có chứa bộ định tuyến và theo D-Link điều kiện này làm giảm đáng kể nguy cơ bị tấn công.

Trước đó, cuối tháng 12/2019, nhiều lỗ hổng nghiêm trọng tồn tại trong các router Wi-Fi Ruckus cũng đã được phát hành bản vá.

Khuyến nghị: Người quản trị và người dùng cần cập nhật các phiên bản mới nhất của các sản phẩm nêu trên để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/nhieu-thiet-bi-dinh-tuyen-d-link-bi-anh-huong-boi-lo-hong-thuc-thi-lenh-tu-xa.13121/

3. Mất 16.000 USD vì add-on trình duyệt

Một người dùng phản ánh đã mất số tiền ảo trị giá 16.000 USD vì cài đặt tiện ích (add-on) trên trình duyệt Google Chrome.

Phần mở rộng "Ledge Secure" trên trình duyệt Google Chrome hóa ra là phần mềm độc hại. Theo quảng cáo, tiện ích này đóng vai trò như ví tiền ảo tích hợp ngay trên Google Chrome.

Tuy nhiên, thay cho chức năng giữ tiền, Ledge Secure lại đánh cắp tiền của người dùng. Hiện chưa rõ có bao người dùng là nạn nhân.

Các báo cáo cho biết Ledge Secure quét máy tính và gửi thông tin cho người tạo ra add-on này. Thông tin đủ ở mức kẻ tạo ra Ledge Secure có thể đánh cắp tiền ảo trên máy tính.

Người dùng Twitter có biệt danh "hackedzec" đã lên tiếng xác nhận Ledge Secure đã khiến anh mất 600 ZEC (tiền ảo), tương đương 16.000 USD.

Công ty Ledger của Pháp xác nhận trên Twitter rằng phần mở rộng Ledge Secure không phải add-on hợp pháp và khuyến cáo người dùng không cài đặt trên máy tính.

Cũng theo Ledger, tin tặc đã tạo ra ứng dụng giả mạo này với mục đích lừa tiền người dùng. Được biết, tình trạng này đã diễn ra cách đây 2 năm. Số người bị lừa tiền cũng như số tiền thất thoát vẫn chưa được xác định.

Google đã gỡ bỏ Ledge Secure khỏi kho ứng dụng Chrome Web Store, và khuyến cáo người dùng kiểm tra lại ví tiền ảo.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng khi cài các add-on của trình duyệt web cần kiểm tra kỹ nguồn gốc nhà phát hành và tính pháp lý trước khi sử dụng để đảm bảo an toàn thông tin.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/mat-16-000-usd-vi-add-on-trinh-duyet-606951.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	Linux	CVE 2019 19966 CVE 2019 19947 CVE 2019 5108 …	Nhóm 07 lỗ hổng trên hệ điều hành Linux (Linux kernel) 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.
2	Apache	CVE 2019 17563 CVE 2019 12418	Nhóm 02 lỗ hổng trên phần mềm Apache (Apache Tomcat 9.0.0.M1) cho phép đối tượng tấn công tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
3	D-link	CVE 2019 6013 CVE 2019 16326 CVE 2014 3136 …	Nhóm 05 lỗ hổng trên thiết bị D link (DBA 1510P, DIR 601B1, DWR 113) cho phép đối tượng thực thi mã tùy ý.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE 2019 19980 CVE 2014 4558 CVE 2014 4539 …	Nhóm 35 lỗ hổng trên một số thành phần của phần mềm Wordpress (Wordpress plugin, Email Subscribers&Newsletters,..) cho phép đối tượng tấn công chèn và thực thi mã tùy ý.	Chưa có thông tin xác nhận và bản vá
5	Huawei	CVE 2019 5276 CVE 2019 5265 CVE 2019 5266 …	Nhóm 09 trên thiết bị Huawei (smart phones, M5 lite 10, USG9500, OceanStor SNS3096 V100R002C01,…) cho phép đối tượng tấn công thu thập thông tin, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
6	PHP	CVE 2019 11046 CVE 2019 11049 CVE 2019 11050 …	Nhóm 06 lỗ hổng trong chương trình viết bằng ngôn ngữ lập trình php (PHP EXIF extension, PHP Directorylterator class…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã lệnh.	Chưa có thông tin xác nhận và bản vá

7	Samsung	CVE 2013 4764 CVE 2013 4763 …	Nhóm 02 lỗ hổng trên thiết bị Samsung (Samsung Galaxy S3/S4) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, chặn các tin nhắn đến và đi theo ý muốn.	Chưa 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	strikotunrev.top
3	hotpassionfinder.com
4	localhost.localdomain
5	pudloxan.com

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.