BẢN TIN NỘI BỘ

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

1. Hacker tiết lộ 4 mã khai thác mới của Microsoft

Chưa đầy 24 giờ sau khi công khai lỗ hổng 0-day chưa được vá trong Windows 10, tin tặc "SandboxEscaper" đã tiết lộ mã khai thác mới cho hai lỗ hổng 0-day chưa được vá khác của Microsoft.

Hai lỗ hổng 0-day mới ảnh hưởng đến dịch vụ Báo cáo Lỗi Windows của Microsoft và Internet Explorer 11.

Lỗ hổng AngryPolarBearBug2

Một trong những lỗ hổng 0-day mới nhất của Microsoft nằm trong dịch vụ Báo cáo Lỗi (Windows Error Reporting) của Windows có thể bị khai thác thông qua danh sách kiểm soát truy cập tùy ý (DACL). Đây là một cơ chế xác định người dùng và các nhóm được phân quyền hoặc không được phân quyền truy cập vào một đối tượng an toàn.

Khi khai thác thành công, kẻ tấn công có thể xóa hoặc chỉnh sửa bất kỳ file Windows nào, bao gồm các file thực thi hệ thống.

Lỗ hổng được đặt tên là AngryPolarBearBug2, là lỗi kế thừa từ lỗ hổng dịch vụ Báo cáo Lỗi Windows được chính hacker SandboxEscape phát hiện vào cuối năm ngoái, có tên AngryPolarBearBug. Lỗ hổng này cho phép kẻ tấn công nội bộ, không được phân quyền có thể ghi đè lên bất kỳ file nào trên hệ thống.

Tuy nhiên, theo hacker SandboxEscaper, lỗ hổng này không dễ khai thác và "có thể mất tới 15 phút để triển khai việc khai thác"

Lỗ hổng vượt qua cơ chế bảo vệ Sandbox trên Internet Explorer 11

Lỗ hổng 0-day thứ hai được SandboxEscaper tiết lộ ảnh hưởng đến trình duyệt web của Microsoft, Internet Explorer 11 (IE11).

Mặc dù thông báo mã khai thác không nêu bất kỳ chi tiết nào về lỗ hổng này, một video minh họa do hacker này đăng tải cho thấy lỗi bắt nguồn từ việc trình duyệt Internet Explorer 11 tồn tại lỗ hổng xử lý file DLL chứa mã độc.

Kẻ tấn công có thể khai thác lỗ hổng này để vượt qua cơ chế bảo vệ sand box của IE và thực thi mã tùy ý với quyền Medium.

Mặc dù đều là lỗ hổng 0-day chưa được vá, nhưng đây là các lỗi không nghiêm trọng. Người dùng có thể chờ đợi các bản cập nhật an ninh vào ngày 11/6 tới từ Microsoft.

Cập nhật quan trọng –Thêm hai lỗ hổng 0-day mới được công bố

Chuyên gia an ninh Gal De Leon từ công ty Palo Alto Networks cho biết AngryPolarBearBug2 không phải là lỗ hổng 0-day. Thực tế lỗ hổng này đã được Microsoft vá vào tháng 5/2019 trong bản cập nhật Patch Tuesday.

Tuy nhiên, SandboxEscaper vừa công khai mã khai thác PoC cho 2 lỗ hổng zero-day mới chưa được vá trong Microsoft Windows, nâng con số lỗ hổng 0-day được tiết lộ lên 4 lỗ hổng.

Mã khai thác đầu tiên vượt qua bản vá Microsoft phát hành cho lỗ hổng leo thang đặc quyền CVE-2019-0841 trong Windows. Lỗ hổng CVE-2019-0841 bắt nguồn từ dịch vụ AppX Deployment (AppXSVC) xử lý không đúng các hard link.

Một công bố khác được SandboxEscaper ghi tên trên GitHub là "Vượt qua Trình cài đặt"

Mặc dù hacker đã đăng tải video minh họa cho việc khai thác cả hai lỗ hổng mới, các nhà nghiên cứu an ninh vẫn chưa xác nhận các tuyên bố trên.

Các chuyên gia an ninh mạng của Bkav khuyến cáo: "Khai thác thành công lỗ hổng bằng mã khai thác PoC do SandboxEscaper cung cấp cho phép kẻ tấn công leo thang đặc quyền quản trị hệ thống, từ đó chiếm quyền kiểm soát hoàn toàn thiết bị. Do vậy, các hệ thống server dịch vụ Windows là đối tượng bị ảnh hưởng nặng nề nhất. Để đảm bảo an toàn cho hệ thống, các quản trị viên cần theo dõi và cập nhật các bản vá mới nhất từ Microsoft càng sớm càng tốt".

Khuyến nghị:

Phòng ATTT khuyến nghị: Quản trị viên và người dùng cần cập nhật ngay các bản vá mới nhất từ Microsoft để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/cap-nhat-hacker-tiet-lo-4-ma-khai-thac-moi-cua-microsoft.12295/

2. Các smart Wi-Fi router Linksys bị phát hiện chứa lỗ hổng rò rỉ thông tin của các thiết bị được kết nối

Hơn 25.000 thiết bị smart Wi-Fi router (bộ định tuyến Wi-Fi thông minh) mang nhãn hiệu nổi tiếng Linksys được cho là đang bị ảnh hưởng bởi một lỗ hổng bảo mật nghiêm trọng, qua đó tiết lộ thông tin cũng như cho phép các truy cập từ xa và không được xác thực tiếp cận được với một loạt dữ liệu nhạy cảm về các thiết bị được kết nối.

Vấn đề này nhìn chung rất giống với sự cố bảo mật phần mềm Linksys SMART WiFi đã từng xuất hiện từ năm 2014, được theo dõi với mã định danh CVE-2014-8244, cho phép "kẻ tấn công từ xa lấy cắp thông tin nhạy cảm hoặc sửa đổi dữ liệu thông qua các hoạt động JNAP trong yêu cầu JNAP/HTTP".

Tuy nhiên, theo báo cáo của đội ngũ các nhà nghiên cứu bảo mật tới từ tổ chức Bad Packet do chuyên gia pháp y máy tính Troy Mursch đứng đầu, thì mặc dù được cho là đã được vá thành công từ khoảng 5 năm trước, nhưng hệ quả mà CVE-2014-8244 để lại thì vẫn còn đó, và ảnh hưởng trực tiếp đến các thiết bị của Linksys như vừa nêu trên. Đáng trách hơn, phía Linksys cũng không hề đưa ra bất cứ khuyến nghị bảo mật cho người dùng hay bất kỳ động thái vá lỗi nào. Tệ hơn, nhóm bảo mật Linksys đã gắn thẻ cho bài báo cáo lỗ hổng của Troy Mursch là "Not applicable/Won't fix" và đóng chủ đề.

Trở lại với báo cáo của Troy Mursch. Ông và các cộng sự đã phát hiện ra có đến 25.617 sản phẩm smart Wi-Fi router của Linksys chứa đựng lỗ hổng khiến chúng dễ bị tổn thương trước các vụ tấn công bảo mật, đồng thời có thể phơi bày hàng loạt thông tin nhạy cảm của các thiết bị được kết nối như:

- Địa chỉ MAC của mọi thiết bị đã từng kết nối với nó (bản ghi lịch sử đầy đủ của tất cả các thiết bị đã từng kết nối chứ không chỉ các thiết bị đang hoạt động).

- Tên thiết bị (chẳng hạn như "QUANTRIMANG-PC" hay "My MacBook Pro").

- Hệ điều hành mà thiết bị đang sử dụng (chẳng hạn như Windows 7, Windows 10 hoặc Android...).

- Các thông số thiết lập mạng WAN, trạng thái tường lửa, các cài đặt cập nhật chương trình cơ sở và cài đặt DDNS.

- Siêu dữ liệu bổ sung được ghi lại như loại thiết bị, số model và mô tả chi tiết về thiết bị đó.

Nghiêm trọng hơn, những thông tin nhạy cảm bị rò rỉ có thể được truy cập dễ dàng bằng cách mở giao diện đăng nhập của bộ định tuyến Linksys Smart Wi-Fi có chứa lỗ hổng bảo mật này trong trình duyệt web, và sau đó chỉ cần nhấp vào các yêu cầu JNAP ở thanh bên trái.

Bên cạnh đó, Troy Mursch cũng đã tuyên bố trong báo cáo của mình rằng "lỗ hổng này có thể cho phép tiết lộ thông tin nhạy cảm mà không cần xác thực và có thể bị khai thác bởi một kẻ tấn công nghiệp dư, có ít kiến thức kỹ thuật".

Nhóm nghiên cứu đã tìm thấy các router smart Wi-Fi của Linksys dễ bị tổn thương đang được sử dụng ở 146 quốc gia, trên hệ thống mạng của 1.998 nhà cung cấp dịch vụ internet, với 11.834 trong số đó được phát hiện ở Hoa Kỳ, 4.942 ở Chile, 2.068 ở Singapore và 1.215 ở Canada.

Đối với các quốc gia còn lại, số lượng router smart Wi-Fi Linksys dễ bị tổn thương hiện có thể truy cập được từ internet không quá nhiều, đa phần ở mức dưới 500 thiết bị, bao gồm: 462 ở Hồng Kông, 440 ở Các Tiểu vương quốc Ả Rập Thống nhất, 280 ở Qatar, 255 Nga, 225 ở Nicaragua và 203 ở Hà Lan. 3.723 thiết bị khác nằm rải rác ở những quốc gia còn lại với số lượng không đáng kể.

Ngoài ra, nhóm của Troy Mursch cũng đã phát hiện ra hàng ngàn smart Wi-Fi router khác của Linksys đang sử dụng mật khẩu quản trị mặc định và hoàn toàn có thể dễ dàng bị những kẻ tấn công tiềm năng truy cập trái phép cũng như chiếm quyền sử dụng ngay lập tức.

Khi một tên tội phạm mạng có quyền kiểm soát một trong số các router này, chúng sẽ có thể thực hiện được những hành vi nguy hiểm như sau:

- Lấy cắp mật khẩu SSID và Wi-Fi dưới dạng văn bản gốc.

- Thay đổi cài đặt DNS nhằm sử dụng máy chủ DNS giả mạo để qua đó chiếm quyền điều khiển lưu lượng truy cập web.

- Mở các cổng trong tường lửa của router để nhắm mục tiêu trực tiếp đến các thiết bị nằm phía sau router đó (ví dụ: 3389/tcp for Windows RDP).

- Sử dụng UPnP để chuyển hướng lưu lượng đi đến thiết bị của kẻ tấn công.

- Tạo tài khoản OpenVPN (các model được hỗ trợ) để định tuyến lưu lượng độc hại thông qua các router bị chiếm đoạt.

- Vô hiệu hóa kết nối internet của router hoặc sửa đổi các chế độ cài đặt khác với mục đích phá hoại.

Tuy nhiên, ông Troy Mursch cũng cho biết mặc dù những động thái của đội ngũ bảo mật Linksys cho thấy rằng ở thời điểm hiện tại họ đang cố gắng né tránh trước yêu cầu khắc phục lỗ hổng bảo mật cực kỳ nguy hiểm trên các sản phẩm của mình, thế nhưng công ty "hiện đã bật tính năng cập nhật firmware tự động". Điều này có nghĩa là Linksys không sớm thì muộn cũng sẽ vá lỗ hổng này trong tương lai. Những thiết bị nằm trong danh sách có chứa lỗ hổng sẽ nhận được bản cập nhật bảo mật cũng như được đặt dưới các quy trình bảo vệ tự động. Sự im lặng của Linksys ở thời điểm hiện tại có lẽ là do công ty vẫn chưa thể tìm ra phương pháp ứng phó tối ưu nhất cho lỗ hổng này.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần cập nhật firmware mới nhất để đảm bảo an toàn thông tin, không bật các tính năng quản trị Smart Wifi Router qua internet.

Link tham khảo: https://quantrimang.com/router-linksys-chua-lo-hong-ro-ri-thong-tin-163696

3. Xu hướng tấn công DDoS bùng phát trở lại

Kết thúc quý 1/2019, số vụ tấn công từ chối dịch vụ (DDoS) tăng 84% so với quý 4/2018. Số cuộc tấn công kéo dài hơn một giờ cùng thời gian trung bình cho mỗi cuộc tấn công cũng đã tăng vượt bậc.

Thông tin nói trên được chia sẻ thông qua số liệu từ báo cáo Kaspersky Lab's DDoS, cho thấy kỹ thuật tấn công DDoS đã cải thiện đáng kể, đồng thời các tin tặc cũng tập trung kéo dài thời gian cho mỗi cuộc tấn công hơn.

Năm ngoái, số vụ tấn công DDoS liên tục giảm, và các chuyên gia của hãng bảo mật Kaspersky Lab cho rằng tội phạm mạng thay vì kiếm lợi từ các cuộc tấn công DDoS thì đã chuyển sự chú ý sang những loại tấn công khác (như khai thác tiền điện tử).

Tuy nhiên, kết thúc quý 1/2019, số liệu cho thấy số lượng các cuộc tấn công DDoS bị phát hiện bởi Kaspersky DDoS Protection đã tăng 84% so với quý 4/2018, nghĩa là tin tặc vẫn đang đặt nhiều chú ý vào những cuộc tấn công này. Đặc biệt khi thị trường cho thuê DDoS (DDoS-for-Hire websites) vừa xuất hiện, số lượng các cuộc tấn công DDoS cũng đã tăng theo cấp số nhân.

Đáng chú ý, có các cuộc tấn công DDoS kéo dài hơn một giờ. Những cuộc tấn công này tăng gấp đôi về số lượng, và thời lượng trung bình cũng tăng 487%. Các chuyên gia từ Kaspersky Lab cho rằng tin tặc đang phát triển kỹ thuật tấn công và hiện có thể thực hiện các cuộc tấn công dài hơn với cơ chế phức tạp hơn.

Kaspersky Lab khuyến nghị các tổ chức nên thực hiện những bước sau để bảo vệ doanh nghiệp khỏi các cuộc tấn công DDoS:

- Đảm bảo rằng tài nguyên web và công nghệ thông tin trong tổ chức có khả năng ứng phó tốt khi lưu lượng truy cập tăng cao.

- Sử dụng các giải pháp chuyên nghiệp như Kaspersky DDoS Protection để bảo vệ tổ chức chống lại các cuộc tấn công. Những giải pháp này có khả năng chống lại tất cả các loại tấn công DDoS bất kể độ phức tạp, sức mạnh hoặc thời lượng của chúng.

Khuyến nghị:

Phòng ATTT khuyến nghị: Quản trị viên cần liên tục giám sát bất thường trong hệ thống để kịp thời xử lý đảm bảo an toàn cho hệ thống.

Link tham khảo: https://thanhnien.vn/cong-nghe/xu-huong-tan-cong-ddos-bung-phat-tro-lai-1084712.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	IBM	CVE-2018-1990 CVE-2019-4204 CVE-2019-4259 CVE-2019-4119 CVE-2018-1975 CVE-2019-4279 ...	Nhóm 06 lỗ hổng trên một số sản phẩm, ứng dụng của IBM (API Connect, DB2 Linux/ Windows, Rational Engineering Lifecycle Manage, IBM SDK, WebSphere Application Server...) cho phép đối tượng tấn công thực hiện thu thập thông tin, khai thác các lỗi tràn bộ đệm để chèn và thực thi mã lệnh, tấn công leo thang.	Đã có thông tin xác nhận và bản vá
2	Cisco	CVE-2019-1649 CVE-2019-1862 CVE-2019-1727 CVE-2019-1728 …..	Nhóm 56 lỗ hổng trong một số sản phẩm của Apache (JMeter, Solr, Qpid Broker-J, Apache Traffic Server) cho phép đối tượng tấn công thực hiện thu thập thông tin, chèn và thực thi mã lệnh trong phạm vi của ứng dụng.	Đã có thông tin xác nhận và bản vá
3	Linux	CVE-2018-7191 CVE-2019-11833 CVE-2019-11884 CVE-2019-11085 ……..	Nhóm 04 lỗ hổng dựa trên một số sản phẩm của Mozilla (Thunderbird…) cho phép kẻ tấn công có quyền truy cập và thực thi vào hệ thống qua nhiều giao thức khác nhau gây ra thiếu dữ liệu.	Đã có thông tin xác nhận và bản vá.
4	Microsoft	CVE-2017-18279 CVE-2017-18156 CVE-2017-18157 CVE-2017-18274 ……	Nhóm lỗ 81 hổng trên một số sản phẩm của Microsoft (edge, Office, Windows 10, chakracore ..) cho phép kẻ tấn công truy cập từ xa, chiếm quyền điều khiển, thực thi mã độc.	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	disorderstatus.ru
2	differentia.ru
3	atomictrivia.ru

4	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
5	1wh1ze3dpc.ru
6	xjpakmdcfuqe.com
7	ei3rvgfk.ru
8	strikotunrev.top
9	kukutrustnet777.info
10	plpanaifheaighai.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.