BẢN TIN NỘI BỘ

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

1. Cisco sửa lỗ hổng nghiêm trọng trong các bộ định tuyến tường lửa và VPN không dây

Theo Cisco, lỗ hổng CVE-2019-1663 cho phép những kẻ tấn công từ xa, không cần xác thực thực thi mã tùy ý.

Cisco khuyến cáo khách hàng nhanh chóng cập nhật các bộ định tuyến VPN không dây và tường lửa, sau khi hãng đã vá một lỗ hổng nghiêm trọng có thể cho phép những kẻ tấn công thực thi mã tùy ý.

Lỗ hổng có điểm CVSS là 9,8 và ảnh hưởng đến các bộ định tuyến sau:

- Tường lửa Cisco RV110W Wireless-N VPN
- Bộ định tuyến đa chức năng không dây Cisco RV130W Wireless-N Multifunction VPN
- Bộ định tuyến VPN không dây Cisco RV215W Wireless-N

Các bộ định tuyến dành doanh nghiệp nhỏ trên được sử dụng để thiết lập kết nối không dây trong các văn phòng nhỏ và văn phòng tại nhà.

Trong khuyến cáo vào ngày 27/2/2018 của Cisco, khi khai thác thành công kẻ tấn công có thể leo thang đặc quyền để thực thi mã tùy ý trên hệ điều hành cơ bản của thiết bị bị ảnh hưởng.

Cụ thể, lỗ hổng tồn tại trong giao diện quản lý dựa trên nền tảng web cho ba mô hình bộ định tuyến.

Lỗ hổng bắt nguồn từ việc giao diện này không kiểm tra chính xác dữ liệu do người dùng gửi đến. Vì vậy, kẻ tấn công có thể gửi các truy vấn HTTP độc hại đến các thiết bị mục tiêu bị ảnh hưởng và cuối cùng thực thi mã trên các thiết bị này. Trầm trọng hơn, kẻ tấn công có thể không cần xác thực và thực hiện từ xa việc tấn công.

Cisco cho biết các bộ định tuyến có tính năng quản lý từ xa được kích hoạt đứng trước nguy cơ bị tấn công từ xa. Tính năng này hiện tắt mặc định, nhưng các quản trị viên có thể kiểm tra tính năng có bật hay không bằng cách chọn Basic Settings>Remote Management trong giao diện web của bộ định tuyến.

Mặc dù Cisco không nêu chi tiết liệu lỗ hổng đã bị khai thác trong thực tế hay chưa, nhưng hãng đã phát hành bản cập nhật firmware cho các thiết bị bị ảnh hưởng nhằm xử lý lỗ hổng.

Các phiên bản phần mềm được vá là:

- Tường lửa RV110W Wireless-N VPN phiên bản 1.2.2.1
- Bộ định tuyến VPN đa chức năng không dây RV130W phiên bản 1.0.3.45
- Bộ định tuyến VPN không dây RV215W phiên bản 1.3.1.1.

Khuyến nghị:

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

Link tham khảo: https://whitehat.vn/threads/cisco-sua-lo-hong-nghiem-trong-trong-cac-bo-dinh-tuyen-tuong-lua-va-vpn-khong-day.12016/

2. Lỗi bảo mật trên 4G và 5G khiến người dùng bị rình rập nghiêm trọng

Các nhà nghiên cứu bảo mật đã phát hiện ba lỗ hổng trong kết nối 5G chỉ sau vài tháng ra mắt, không chỉ có vậy mà thậm chí cả mạng 4G cũng có. Với ba lỗ hổng này, những kẻ xấu có thể chặn cuộc gọi và dò tìm vị trí của người dùng một cách dễ dàng.

Đầu tiên và quan trọng nhất chính là Torpedo, dựa trên một lỗ hổng trong giao thức phân trang mà thông báo cho điện thoại các cuộc gọi và tin nhắn đến. Nếu bạn bắt đầu gọi và hủy một số cuộc gọi trong một khoảng thời gian ngắn, bạn có thể gửi tin nhắn phân trang mà không báo cho thiết bị biết cuộc gọi tới. Việc này không chỉ cho phép bạn định vị thiết bị mà còn mở ra thêm đường cho hai cuộc tấn công tin tặc khác.

Một trong hai đường mới được mở ra là Piercer, cho phép bạn xác định số IMSI duy nhất được đính kèm với người dùng. Trên 4G, một cuộc tấn công bẻ khóa vào số IMSI có thể đoán số IMSI thông qua tấn công theo phương thức Brute Force Attack trên cả 4G và 5G.

Điều này giúp các hacker có thể theo dõi các cuộc gọi và thông tin vị trí thông qua các thiết bị như Stingrays ngay cả khi bạn có một chiếc điện thoại 5G hoàn toàn mới. Torpedo cũng có thể chèn hoặc chặn các tin nhắn như cảnh báo Amber.

Các lỗ hổng này có khả năng ảnh hưởng đến hầu hết mọi mạng 4G hoặc 5G trên thế giới, mặc dù vậy thì mức độ ảnh hưởng rất khác nhau. Tất cả bốn nhà mạng lớn nhất của Mỹ (AT & T, Sprint, T-Mobile và Verizon) đều dễ bị Torpedo, trong khi một mạng không tên cũng có thể trở thành con mồi của Piercer. Như vậy thì thậm chí cả Việt Nam cũng không hề nằm ngoài danh sách.

Các lỗ hổng này có thể vá được, nhưng sẽ mất khá lâu vì Torpedo và bẻ khóa IMSI cần phải có giải pháp trực tiếp từ ngành công nghiệp mạng tiêu chuẩn, còn Piercer thì đòi hỏi các nhà mạng phải ra tay để vá. Bạn cũng không cần quá lo lắng, vì đây chỉ là mô tả từ các nhà nghiên cứu mà thôi, còn cách để thực hiện thì vẫn được giữ bí mật tuyệt đối.

Link tham khảo: https://whitehat.vn/threads/loi-bao-mat-tren-4g-va-5g-khien-nguoi-dung-bi-rinh-rap-nghiem-trong.12006/

3. Lỗ hổng WinRAR bị lợi dụng để tấn công máy tính Windows

WinRAR là một ứng dụng nén tệp Windows phổ biến với 500 triệu người dùng trên toàn thế giới. Lỗ hổng "Absolute Path traversal" nghiêm trọng (CVE-2018-20250) đã được phát hiện gần đây giúp kẻ tấn công có thể tạo ra các file thực thi trong các thư mục Windows Startup, nơi tệp sẽ tự động chạy trong lần khởi động lại tiếp theo. Lỗi này được cho là có ảnh hưởng tới tất cả các phiên bản WinRAR được phát hành trong suốt 19 năm qua.

Để khai thác thành công lỗ hổng và kiểm soát hoàn toàn các máy tính mục tiêu, tất cả những gì kẻ tấn công cần làm chỉ là thuyết phục người dùng mở tệp nén độc hại được tạo thủ công bằng WinRAR.

Các nhà nghiên cứu bảo mật tại 360TIC đã phát hiện một chiến dịch email malspam đang phát tán tệp lưu trữ RAR độc hại khai thác lỗ hổng WinRAR mới nhất để cài đặt phần mềm độc hại trên các máy tính chạy phiên bản phần mềm tồn tại lỗ hổng.

Đầu tiên, phần mềm độc hại được gửi qua thư để khai thác lỗ hổng WinRAR, sau đó tạo cửa hậu (backdoor) bằng MSF [Microsoft Solutions Framework] và được WinRAR ghi vào thư mục khởi động nếu UAC bị tắt.

Như được hiển thị trong ảnh chụp màn hình do các nhà nghiên cứu chia sẻ, khi mở bằng phần mềm WinRAR và chạy với đặc quyền của quản trị viên hoặc UAC bị vô hiệu hóa, phần mềm độc hại (vốn được thiết kế để lây nhiễm máy tính mục tiêu và tạo ra một backdoor) tạo ra các tệp tin exe độc hại (CMSTray.exe) vào thư mục Windows Startup.

Nếu UAC được bật, mã độc sẽ không thể lây nhiễm vào vào thư mục C:\ProgramData, do đó không gây ảnh hưởng tới máy tính.

Cách tốt nhất để bảo vệ bạn khỏi các cuộc tấn công này là cập nhật phần mềm bằng cách cài đặt phiên bản WinRAR mới nhất càng sớm càng tốt và tránh mở các tệp nhận được từ các nguồn không xác định.

Do nhóm WinRAR đã mất quyền truy cập vào mã nguồn cho thư viện UNACEV2.DLL tồn tại lỗ hổng từ năm 2005, nên thay vì khắc phục sự cố, đội ngũ WinRAR đã phát hành phiên bản WINRar 5.70 beta 1 không hỗ trợ định dạng DLL và ACE. Việc này giúp khắc phục được lỗi đã công bố, nhưng đồng thời cũng loại bỏ tất cả hỗ trợ của ACE khỏi WinRAR.

Khuyến nghị:

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

Link tham khảo: https://securitydaily.net/lo-hong-winrar-bi-loi-dung-de-tan-cong-may-tinh-windows/

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	D-Link	CVE-2019-7736 CVE-2019-8312 CVE-2019-8319 ...	Nhóm 10 lỗ hổng trên firmware nột số dòng thiết bị của Dlink (600M C1 3.04, DIR-878, DIR-823G, DIR-878) cho phép đối tượng tấn công truy cập trực tiếp vào trang wan.htm thay đổi thông tin cấu hình trên thiết bị, chèn và thực thi lệnh tùy ý để chiếm quyền kiểm soát thiết bị.	Chưa có thông tin xác nhận và bản vá
2	Google Android	CVE-2018-11962 CVE-2018-9587 CVE-2018-9592 ...	Nhóm 23 lỗ hổng trên hệ điều hành Android cho phép đối tượng tấn công thực hiện để thu thập thông tin, chèn và thực thi mã lệnh, tấn công leo thang.	Đã có thông tin xác nhận và bản vá
3	Joomla	CVE-2019-7739 CVE-2019-7741 CVE-2019-7744 ….	Nhóm 06 lỗ hổng trong phần mềm quản trị nội dung Joomla cho phép đối tượng tấn công thực hiện khai thác lỗi XSS thông qua nhiều thành phần khác nhau	Đã có thông tin xác thực và bản vá
4	IBM	CVE-2019-4059 CVE-2018-1727 CVE-2017-1695 ...	Nhóm 05 lỗ hổng trên một số sản phẩm, ứng dụng của IBM (QRadar SIEM, InfoSphere Information Server, Rational ClearCase) cho phép đối tượng tấn công thực hiện một số hình thức tấn công gồm: giải mã dữ liệu (do sử dụng giải thuật mã hóa yếu), thu thập thông tin quan trọng, bao gồm cả cơ sở dữ liệu lưu trữ mật khẩu thông qua các connector	Đã có thông tin xác nhận và bản vá
5	SAP	CVE-2019-0265 CVE-2019-0258 CVE-2019-0251	Nhóm 12 lỗ hổng trên một số sản phẩm, ứng dụng của SAP gồm (ABAP Platform, BusinessObjects, Disclosure	Đã có thông tin xác nhận và bản vá

		...	Management, Fiori Launchpad, HANA Extended Application Services, SAP Manufacturing Integration and Intelligence…) cho phép đối tượng tấn công thực hiện khai thác lỗi XSS, thu thập thông tin, đưa tập tin độc hại lên hệ thống, tấn công leo thang	
6	Winrar	CVE-2018-20250	Ảnh hưởng tới phiên bản Winrar 5.60 và các phiên bản trước đó. Trong tuần 6 cũng có lỗ hổng CVE-2018-20253 cho phép thực thi mã lệnh. Ảnh hưởng tới phiên bản WinRAR 5.70 Beta 1 và các phiên bản trước đó.	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	plpanaifheaighai.com
2	n.hmiblgoja.ru
3	ajkeahkcueafuiaeuf.ru
4	mokoaehaeihgiaheih.ru
5	kisssweetchick.com
6	mel.cloudcontentsmak.com
7	43trfdsds.com
8	strikotunrev.top
9	bszotsjovih.com
10	iuefgauiaiduihgs.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.