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

1. Adobe vá lỗ hổng ColdFusion bị khai thác trên thực tế

Lỗ hổng zero-day, CVE-2019-7816 là vấn đề qua mặt cơ chế giới hạn tải file dẫn đến thực thi mã tùy ý trong dịch vụ ColdFusion.

Lỗ hổng xuất hiện trong ColdFusion 11, ColdFusion 2016 và ColdFusion 2018. Ngoài việc cài đặt các bản cập nhật sớm nhất có thể, Adobe còn khuyến cáo người dùng áp dụng các cài đặt an ninh theo hướng dẫn trên trang của ColdFusion.

Theo Adobe: "Kỹ thuật tấn công này yêu cầu phải tải mã thực thi lên thư mực truy cập web (web-accessible directory), sau đó thực thi mã thông qua truy vấn HTTP. Việc giới hạn các yêu cầu đến thư mục upload file lưu trữ sẽ giảm thiểu nguy cơ bị tấn công".

Chưa có thông tin chi tiết về kỹ thuật của các cuộc tấn công khai thác lỗ hổng này.

ColdFusion không phải là lỗ hổng duy nhất bị khai thác gần đây. Trước đó vào tháng 11 năm ngoái, Volexity cũng tiết lộ lỗ hổng CVE-2018-15961 Adobe vá vào tháng 09, bị khai thác bởi một nhóm tấn công có chủ đích tại Trung Quốc, tải một webshell đời cũ lên China Chopper (công cụ quản lý Webshell) đến các máy chủ dính lỗ hổng.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người sử dụng cần cập nhật phiên bản mới nhất của Adobe ColdFusion để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/adobe-va-lo-hong-coldfusion-bi-khai-thac-tren-thuc-te.12018/

2. Google: Hacker kết hợp 2 lỗ hổng 0-day trên Chrome và Windows để tấn công người dùng

Hai lỗ hổng được đội nghiên cứu của Google báo cáo lần đầu ngày 27/2. Để khắc phục lỗ hổng Chrome CVE-2019-5786, Google đã phát hành bản cập nhật tự động cho tất cả các nền tảng Chrome vào ngày 1/3. Người dùng được khuyến cáo kiểm tra Chrome trên thiết bị của mình đã được cập nhật lên phiên bản 72.0.3626.121 trở lên hay chưa.

Lỗ hổng trên Microsoft Windows là lỗ hổng leo thang đặc quyền nội bộ, tồn tại trong kernel driver win32k.sys của Windows và có thể bị hacker lợi dụng để vượt qua cơ chế an ninh sandbox.

Đội nghiên cứu của Google tin rằng lỗ hổng này chỉ có thể khai thác được trên Windows 7 nhờ các bản vá lỗi gần đây được cập nhật trên các phiên bản Windows mới hơn. Đến nay, các chuyên gia mới chỉ phát hiện hoạt động khai thác trên hệ thống Windows 7 32-bit.

Căn cứ vào chính sách tiết lộ lỗ hổng của Google, sau khi phát hiện lỗ hổng, đội nghiên cứu đã thông báo tới Microsoft và tới ngày 7/3 mới công bố rộng rãi vì đây là

một lỗ hổng nghiêm trọng và đang bị khai thác trong các cuộc tấn công có chủ đích. Lỗ hổng Windows chưa được vá vẫn có thể bị khai thác để leo thang đặc quyền hoặc kết hợp với lỗ hổng trình duyệt khác để vượt qua cơ chế bảo vệ sandbox. Microsoft cho biết hãng đang tìm cách xử lý vấn đề.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng nên nâng cấp lên Windows 10 nếu vẫn đang chạy phiên bản Windows cũ hơn và cập nhật từ Microsoft ngay khi có bản vá để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/google-hacker-ket-hop-2-lo-hong-0-day-tren-chrome-va-windows-de-tan-cong-nguoi-dung.12032/

3. Lỗ hổng nghiêm trọng trong ứng dụng SHAREit

SHAREit là một ứng dụng chia sẻ tệp phổ biến cho Android, iOS, Windows và Mac với hơn 1,5 tỷ người dùng trên toàn thế giới. SHAREit được thiết kế để giúp mọi người chia sẻ video, nhạc, tệp và ứng dụng trên nhiều thiết bị khác nhau.

Tuy nhiên, ứng dụng SHAREit trên Android đang gây hoang mang cho hơn 500 triệu người dùng của mình khi mới đây nhóm nghiên cứu RedForce đã phát hiện ra lỗ hổng xác thực nghiêm trọng trong ứng dụng chuyển tập tin và tải xuống tệp tùy ý.

Máy chủ SHAREit lưu trữ nhiều dịch vụ thông qua các cổng khác nhau trên một thiết bị, nhưng các nhà nghiên cứu đã phân tích hai dịch vụ được chỉ định bao gồm Command Chanel (chạy trên Cổng 55283) và Download Chanel (chạy trên Cổng 2999).

Command Chanel là kênh TCP thông thường nơi ứng dụng trao đổi tin nhắn với các phiên bản SHAREit khác đang chạy trên các thiết bị khác bằng kết nối Socket, bao gồm nhận dạng thiết bị, xử lý yêu cầu truyền tệp và kiểm tra chất lượng kết nối.

Download Chanel là máy chủ HTTP của ứng dụng SHAREit, chủ yếu được các khách hàng sử dụng để tải xuống các tệp được chia sẻ.

Khi 'người nhận' xác minh rằng tệp không bị trùng lặp, nó sẽ chuyển đến Download Chanel và tìm tệp đã gửi bằng thông tin từ thông báo điều khiển trước đó.

Các nhà nghiên cứu phát hiện ra rằng khi người dùng không hợp lệ cố gắng truy cập một trang không tồn tại, thay vì hiển thị trang 404 thông thường, ứng dụng SHAREit sẽ phản hồi với trang trống kèm theo mã trạng thái 200 và thêm người dùng vào các thiết bị được nhận dạng, cuối cùng xác thực một người dùng trái phép.

Theo các nhà nghiên cứu, việc khai thác lỗ hổng SHAREit rất đơn giản, chỉ cần gửi request đến máy chủ của SHAREIT,

ví dụ: url http://shareit_sender_ip:2999/DontExist, biến nó thành phương thức xác thực kỳ lạ và đơn giản nhất từ trước đến nay.

Các nhà nghiên cứu cũng nhận thấy rằng khi yêu cầu tải xuống được bắt đầu, máy khách SHAREit sẽ gửi yêu cầu GET đến máy chủ HTTP của người gửi, trông giống như URL sau:

http://shareit_sender_ip:2999/download?metadatatype=photo&metadataid=1337&filetype=thumbnail&msgid=c60088c13d6

Vì ứng dụng SHAREit không xác thực tham số ‘msgid’ (một mã định danh duy nhất được tạo cho mỗi yêu cầu khi người gửi bắt đầu tải xuống), điều này cho phép một máy khách độc hại có phiên hợp lệ có thể tải xuống bất kỳ tài nguyên nào bằng cách tham chiếu trực tiếp mã định danh của nó.

Các lỗ hổng có thể bị kẻ tấn công khai thác trên một mạng WiFi được chia sẻ. Các phiên bản SHAREit chứa lỗ hổng sẽ tạo ra một điểm truy cập Wi-Fi mở, không chỉ cho phép kẻ tấn công chặn lưu lượng truy cập (vì nó sử dụng HTTP) giữa hai thiết bị, mà còn có quyền truy cập không hạn chế vào bộ lưu trữ trên thiết bị của nạn nhân.

Ngay khi phát hiện ra lỗ hổng này, các nhà nghiên cứu trong nhóm RedForce đã nhiều lần liên hệ với SHAREit vào đầu tháng 1 năm 2018 nhưng không nhận được bất cứ phản hồi nào. Cho đến đầu tháng 2, khi các nhà nghiên cứu cảnh báo sẽ công bố chi tiết lỗ hổng cho công chúng sau 30 ngày thì mới nhận được phản hồi từ SHAREit.

Tuy vậy, sau đó SHAREit đã âm thầm vá các lỗ hổng vào tháng 3 năm 2018, mà không cung cấp cho các nhà nghiên cứu các phiên bản vá chính xác của ứng dụng Android, ID CVE cũng như không có bất kỳ bình luận nào cho lỗ hổng.

Sau khi dành đủ thời gian cho người dùng cập nhật ứng dụng SHAREit của họ, các nhà nghiên cứu trong nhóm RedForce đã công bố chi tiết kỹ thuật về các lỗ hổng, cùng với khai thác PoC, DUMBit! Trên trang web GitHub.

Các lỗ hổng ảnh hưởng đến ứng dụng SHAREit cho Android <= phiên bản 4.0.38. Và nếu bạn đang sử dụng ứng dụng SHAREit trên nền tảng Android thì bạn cần cập nhật ngay phiên bản mới nhất của ứng dụng này trên Google Play càng sớm càng tốt.

Khuyến nghị:

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

Link tham khảo: https://securitydaily.net/lo-hong-nghiem-trong-trong-ung-dung-shareit/

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	GNU Glibc	CVE-2018-20796 CVE-2019-9169	Nhóm 04 lỗ hổng trong bộ thư viện GNU C Library (bộ thư viện mặc định trên hầu hết các hệ điều hành Linux) cho phép khai thác lỗi tràn bộ đệm để thực thi mã lệnh tùy ý trong phạm vi của ứng dụng, hay thực hiện tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
2	Cisco	CVE-2019-1663 CVE-2019-1674 CVE-2019-1689 ...	Nhóm 04 lỗ hổng trên một số sản phẩm, ứng dụng của Cisco (Router (RV110W, RV130W, & RV215W), IP Phone (SPA112, SPA525, SPA5x5), Webex Meetings Desktop App, Webex Productivity Tools) cho phép đối tượng tấn công thực hiện một số hình thức tấn công như nghe lén, ghi đè tập tin độc lại lên hệ thống, chèn và thực thi mã lệnh từ xa	Đã có thông tin xác nhận và bản vá
3	D-Link	CVE-2019-9123 CVE-2019-9124 CVE-2019-9125	Nhóm 05 lỗ hổng phát hiện trên một số dòng D-link (DIR-825 Rev.B 2.10, DIR-878 1.12B01) cho phép đối tượng tấn công truy cập vào thiết bị sử dụng mật khẩu trống của tài khoản mặc định, chèn và thực thi mã lệnh từ xa để chiếm quyền kiểm soát thiết bị	Chưa có thông tin xác thực và bản vá
4	Google Android	CVE-2019-1986 CVE-2019-1987 CVE-2019-1988 ...	Nhóm 14 lỗ hổng trên một số thành phần của hệ điều hành Android cho phép đối tượng tấn công chèn và thực thi mã lệnh, tấn công leo thang và truy cập trái phép vào thiết bị.	Đã có thông tin xác nhận và bản vá.02 lỗ hổng đã có mã khai

				thác
5	Firefox	CVE-2018-12390 CVE-2018-12391 CVE-2018-12392 ...	Nhóm 25 lỗ hổng trên trình duyệt Firefox cho phép đối tượng tấn công thực hiện thực thi mã lệnh tùy ý, tấn công leo tháng, vượt qua cơ chế bảo mật để thực hiện những hành vi trái phép trên thiết bị. Ảnh hưởng tới các phiên bản Firefox < 63, Firefox ESR < 60.3	Đã có thông tin xác nhận và bản vá
6	PHP	CVE-2019-9021 CVE-2019-9022 CVE-2019-9024 ...	Nhóm 06 lỗ hổng trên nhiều phiên bản PHP cho phép đối tượng tấn công khai thác lỗi tràn bộ đệm để thực thi mã lệnh, thu thập thông tin trái phép trên hệ thống.	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	mel.cloudcontentsmak.com 69 6
6	iuefgauiaiduihgs.com
7	43trfdsds.com
8	strikotunrev.top
9	bszotsjovih.com
10	d3s1.me

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.