**BẢN TIN NỘI BỘ**

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

## 1. Malware Android lợi dụng cảm biến chuyển động ẩn nấp trên điện thoại

Khi Google và các nhà nghiên cứu càng nâng cao mức độ bảo mật cho Play Store thì những kẻ xấu lại càng tinh vi hơn.

Theo AndroidAuthority, hiện trên Play Store đã xuất hiện những ứng dụng cài đặt sẵn mã độc, và chúng chỉ triển khai hoạt động khi ứng dụng nhận diện chuyển động từ smartphone.

Hầu hết những nhóm nghiên cứu bảo mật sử dụng chương trình giả lập Android để kiểm tra malware, và đó không phải là smartphone thật. Các chương trình giả lập thường không được thiết kế để mô phỏng chuyển động, vì điều này bị cho là không cần thiết. Chính vì vậy, tin tặc đã tìm ra cách mới để malware lách qua chúng mà không bị phát hiện rồi dễ dàng xâm nhập vào điện thoại.

Công ty bảo mật Trend Micro đã phát hiện ra cách thức hoạt động này trên hai ứng dụng BatterySaverMobi và Currency Converter. Cả hai ứng dụng đã bị gỡ bỏ khỏi Google Play Store. May mắn thay, BatterySaverMobi có ít hơn 5 ngàn lượt tải nên chưa trở thành vấn đề quá lớn.

Chi tiết hơn, mã độc trên hai ứng dụng đó là một loại malware đánh cắp thông tin tên Anubis. Khi chúng được kích hoạt bên trong, tin tặc sẽ sử dụng các lệnh yêu cầu và phản hồi thông qua ứng dụng Twitter và Telegram để xác định ra dòng lệnh giúp kiểm soát hệ thống.

***Khuyến nghị:***

Phòng ATTT khuyến nghị: Người dùng Android cần gỡ bỏ ngay lập tức 2 ứng dung BatterySaverMobi và Currency Converter và chỉ cài đặt các ứng dụng tin tưởng để bảo đảm an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/malware-android-loi-dung-cam-bien-chuyen-dong-an-nap-tren-dien-thoai-1045240.html

## 2. Cisco vá các lỗ hổng trong Webex, SD-WAN và các sản phẩm khác

Cisco vừa thông báo tới khách hàng các bản cập nhật an ninh cho một số sản phẩm của công ty, bao gồm SD-WAN, Webex, Firepower, IoT Field Network Director, Identity Services Engine và các bộ định tuyến cho doanh nghiệp nhỏ.

Chỉ có một lỗ hổng nguy hiểm là CVE-2019-1651 ảnh hưởng đến thành phần vContainer trong giải pháp SD-WAN của Cisco. Sau khi đăng nhập thành công, kẻ tấn công có thể khai thác lỗ hổng để tấn công DoS và thực thi mã tùy ý với quyền root. Để khai thác lỗ hổng này đòi hỏi phải gửi một file đặc biệt để gây ra lỗi tràn bộ đệm.

Một số lỗ hổng khác, được đánh giá là mức độ nghiêm trọng cao, dựa trên điểm số CVSS, đã được Cisco xử lý trong SD-WAN. Các lỗ hổng có thể bị khai thác để vượt qua cơ chế xác thực, leo thang đặc quyền trên thiết bị và ghi đè lên các file tùy

ý. Tuy nhiên, việc khai thác đòi hỏi kẻ tấn công phải xác thực thành công trên hệ thống mục tiêu.

Cisco cũng vá một số lỗ hổng nghiêm trọng khác trong các sản phẩm Webex, bao gồm lỗ hổng có thể khai thác để thực thi lệnh trong ứng dụng client của Webex Teams và năm lỗi thực thi mã trong các phiên bản Windows của Webex Network Recording Player và Webex Player.

Hai lỗ hổng nghiêm trọng cũng đã được vá trong các bộ định tuyến RV320 và RV325 của Cisco. Một trong hai lỗ hổng trên cho phép kẻ tấn công từ xa không cần xác thực có thể lấy được thông tin nhạy cảm, trong khi lỗ hổng còn lại có thể bị khai thác để chèn lệnh tùy ý, nhưng việc khai thác đòi hỏi phải có đặc quyền của quản trị viên.

RedTeam Pentesting, công ty đã tìm ra các lỗ hổng của bộ định tuyến, đã công bố khuyến cáo tới người dùng.

Đối với sản phẩm tường lửa Firepower, Cisco đã giải quyết một lỗ hổng vượt qua an ninh và lỗ hổng DoS có thể bị khai thác từ xa mà không cần xác thực. Một lỗ hổng DoS cũng đã được giải quyết trong sản phẩm IoT Field Network Director của Cisco.

Cuối cùng, một lỗ hổng leo thang đặc quyền có thể bị khai thác để chiếm quyền "super admin" (quản trị cao cấp) đã được xử lý trong Identity Services Engine (hệ thống kiểm soát thiết bị truy cập vào mạng).

Cisco cho biết không có dấu hiệu nào cho thấy bất kỳ lỗi nào được vá trong tuần này đã bị khai thác với mục đích xấu. Nhiều lỗ hổng đã được tìm thấy bởi chính Cisco.

***Khuyến nghị:***

Phòng ATTT khuyến nghị: Người dùng và quản trị viên cần cập nhật phiên bản mới nhất của các thiết bị nêu trên để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/cisco-va-cac-lo-hong-trong-webex-sd-wan-va-cac-san-pham-khac.11946/

## 3. Ứng dụng quản lý tập tin ES FILE EXPLORER gặp lỗi lộ dữ liệu

ES File Explorer là một trong những ứng dụng phổ biến nhất khi nói về quản lý tập tin trên điện thoại Android. Tuy nhiên, lỗ hổng mới nhất trên nó đã đặt dấu hỏi cho sự tin tưởng mà nhiều người dùng đặt vào ứng dụng này.

Theo Howtogeek, lỗ hổng được nhắc đến khiến tập tin trong thiết bị bạn bị lộ ra cho bất cứ ai đang sử dụng chung hệ thống mạng – khi bạn mở ứng dụng này dù chỉ một lần. Nhà nghiên cứu Elliot Alderson đã phát hiện ra lỗi và đăng tải thông tin lên Twitter.

Cụ thể, ES để một cổng kết nối mở trên điện thoại sau khi bạn truy cập vào ứng dụng. Điều này cho phép những người đang sử dụng cho kết nối mạng với bạn có thể truy cập vào hệ thống dữ liệu điện thoại. Nguy hiểm hơn, kẻ xấu có khả năng sử dụng cổng kết nối mở đó để cài vào một mã độc và dễ dàng tải về tất cả dữ liệu lẫn thông tin trên điện thoại.

Nhóm phát triển ứng dụng thông báo họ đã biết vấn đề và khắc phục nó: "Chúng tôi đã sửa lỗ hổng này và đưa ra bản cập nhật, hiện chờ được Google chấp nhận". ES File Explorer sở hữu hơn 100 triệu lượt tải.

***Khuyến nghị:***

Phòng ATTT khuyến nghị: Người dùng cần cập nhật phiên bản mới nhất ứng dụng **ES FILE EXPLORER** để đảm bảo an toàn thông tin.

Link tham khảo: https://securitybox.vn/7252/ung-dung-quan-ly-tap-tin-es-file-explorer-gap-loi-lo-du-lieu/

## 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 | Apple | CVE-2018-4189<br>CVE-2018-4258<br>CVE-2018-4182<br>… | Nhóm 29 lỗ hổng trên một số sản phẩm hệ điều hành của Apple (iOS, macOS, tvOS) cho phép đối tượng tấn công thực hiện khai thác lỗi tràn bộ đệm, thực thi mã lệnh từ xa, thu thập thông tin nhạy cảm trên hệ thống, tấn công leo thang. | Đã có thông tin xác nhận và bản vá |
| 2 | Oracle | CVE-2019-2437<br>CVE-2019-2511<br>CVE-2019-2432<br>..... | Nhóm 137 lỗ hổng trên một số sản phẩm, ứng dụng của Oracle (Solaris, VM VirtualBox, Enterprise Manager Products Suite, E-Business Suite, MySQL ...) cho phép đối tượng tấn công thực hiện truy cập trái phép vào hệ thống thông qua kết nối HTTP, SOAP để thu thập thông tin quan trọng trên hệ thống; thực thi mã. | Đã có thông tin xác nhận và bản vá. |
| 3 | IBM | CVE-2018-1956<br>CVE-2018-1967<br>CVE-2018-1969<br>... | Nhóm 05 lỗ hổng trên một số sản phẩm, ứng dụng IBM cho phép đối tượng tấn công thực hiện thu thập thông tin, đánh cắp thông tin xác thực dựa trên Cookie, khai thác lỗi XSS, đưa tập tin trái phép vào hệ thống và thực thi đoạn mã, tập tin độc hại. | Đã có thông tin xác nhận và bản vá. |
| 4 | Bind | CVE-2017-3137<br>CVE-2017-3142<br>CVE-2017-3143<br>.... | Nhóm 11 lỗ hổng trên dịch vụ Bind và DHCP cho phép đối tượng tấn công can thiệp vào việc cập nhật bản ghi DNS, là cho hệ thống phân giải tên miền không được chính xác, hoặc gây lỗi. | Đã có thông tin xác nhận và bản vá Một số đã có mã khai thác |

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

| **STT** | **Tên miền/IP** |
|---|---|
| 1 | www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com |
| 2 | www.cityofangelsmagazine.com |
| 3 | dqrzxapnw.info |
| 4 | caarmelcollege.org |
| 5 | osheoufhusheoghuesdl.com |
| 6 | msjbsiq.com |
| 7 | 6ae79845b2.pw |
| 8 | www.corpnox-technologie.fr |
| 9 | nlcfoundation.org |
| 10 | ahmedfahmy.name |

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.