BẢN TIN NỘI BỘ

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

1. Cisco vá các lỗi nghiêm trọng trong HyperFlex và Prime Infrastructure

Cisco vừa phát hành các bản vá cho hơn mười lỗ hổng trên các sản phẩm của hãng, bao gồm các lỗ hổng nghiêm trọng trong HyperFlex, Prime Infrastructure và Prime Collaboration Assurance.

Hai lỗi nghiêm trọng đã được xử lý trong phần mềm HyperFlex. Đây là các lỗi chèn lệnh trong trình quản lý dịch vụ và lỗ hổng chiếm truy cập root trong dịch vụ hxterm của phần mềm.

Nguyên nhân của 2 lỗ hổng lần lượt do việc kiểm tra tính hợp lệ của đầu vào và kiểm soát xác thực không chính xác. Các lỗ hổng có thể cho phép kẻ tấn công chạy các lệnh với quyền root hoặc chiếm quyền truy cập root vào tất cả các nút (node) thành viên của HyperFlex.

Hai lỗ hổng CVE-2018-15380 và CVE-2019-1664 đều tồn tại trên các bản phát hành phần mềm HyperFlex trước 3.5 (2a).

Một lỗi nghiêm trọng khác trong giải pháp Prime Infrastructure (PI) được xử lý trong tuần này là lỗi xác thực chứng chỉ trong tính năng tích hợp Identity Services Engine. Kẻ tấn công từ xa không cần xác thực có thể khai thác lỗ hổng để thực hiện tấn công man-in-the-middle vào tunnel Secure Sockets Layer (SSL) được thiết lập giữa ISE và PI.

Lỗ hổng CVE-2019-1659 bắt nguồn từ việc xác thực không chính xác chứng chỉ SSL của máy chủ khi thiết lập tunnel SSL với ISE. Lỗ hổng tác động đến phần mềm Prime Infrastructure phiên bản từ 2.2 đến 3.4.0 khi máy chủ PI được tích hợp với ISE, được tắt mặc định.

Một lỗ hổng có nguy cơ cao khác được tìm thấy trong dịch vụ Báo cáo Chất lượng giọng nói (QOVR) của phần mềm quản lý giọng nói và video Prime Collaboration Assurance (PCA) trước 12.1 SP2. Lỗ hổng CVE-2019-1662 bắt nguồn từ việc kiểm soát xác thực không chính xác và có thể cho phép kẻ tấn công từ xa không cần xác thực truy cập vào hệ thống như một người dùng hợp lệ.

Dịch vụ TFTP của phần mềm Cisco Series Convergence System 1000 Series tồn tại lỗ hổng CVE-2019-1681. Đây là lỗ hổng nguy cơ cao khai thác qua directory traversal và hacker từ xa có thể khai thác lỗ hổng để lấy các file tùy ý từ thiết bị mục tiêu. Lỗi ảnh hưởng đến Bản phát hành Phần mềm IOS XR trước phiên bản 6.5.2 của sản phẩm Network Convergence System 1000 Series khi bật dịch vụ TFTP.

Cisco cũng đã phát hành các bản vá cho 11 lỗ hổng nghiêm trọng mức độ trung bình ảnh hưởng đến Webex Meetings Online, Webex Teams, phần mềm Internet of Things Field Network Director (IoT-FND), HyperFlex, Firepower Threat Defense, Firepower 9000 Series Firepower 2-Port 100G Double-Width Network Module Queue Wedge, Unity Connection, IP Phone 7800, 8800 Series, SPA112, SPA525 và SPA5X5 Series IP Phones.

Ngoài ra, Cisco cũng cho biết trong quá trình điều tra xác định các sản phẩm vẫn bị ảnh hưởng, hãng này cũng phát hiện lỗ hổng CVE-2019-5736 ảnh hưởng đến nền tảng Cisco Container Platform và ứng dụng dựa trên đám mây Cisco Defense Orchestrator. Mã khai thác lỗ hổng này đã được công bố.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người quản trị 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-va-cac-loi-nghiem-trong-trong-hyperflex-va-prime-infrastructure.11998/

2. Hacker sử dụng link độc khai thác lỗi trên Facebook

Một nhà nghiên cứu vừa phát hiện ra lỗ hổng bảo mật nghiêm trọng nằm trong quyền chứng thực web (CSRF) của nền tảng phương tiện truyền thông xã hội phổ biến nhất hiện nay, lỗi này có thể cho phép kẻ tấn công chiếm đoạt tài khoản Facebook bằng cách lừa người dùng click vào liên kết.

Nhà nghiên cứu có nickname "Samm0uda", đã phát hiện ra lỗ hổng sau khi phát hiện ra một điểm cuối (facebook.com/comet/dialog_DONOTUSE/) có thể bị khai thác để vượt qua cơ chế bảo vệ của CSRF và chiếm đoạt tài khoản của người dùng.

"Điều này có thể là do điểm cuối có lỗi và hacker lợi dụng để tấn công, kết hợp với các tham số và thực hiện yêu cầu POST đến điểm cuối đó sau khi thêm tham số fb_dtsg", nhà nghiên cứu nói trên blog của mình

"Ngoài ra, điểm cuối này nằm dưới tên miền chính www.facebook.com, giúp kẻ tấn công dễ dàng hơn để lừa các nạn nhân của mình truy cập URL".

Tất cả những gì kẻ tấn công cần làm là lừa các nạn nhân nhấp vào URL Facebook được tạo đặc biệt, được thiết kế riêng để thực hiện nhiều hành động như đăng bất cứ điều gì trên dòng thời gian, thay đổi hoặc xóa ảnh hồ sơ của nạn nhân và thậm chí lừa người dùng xóa toàn bộ tài khoản Facebook.

Việc chiếm quyền kiểm soát hoàn toàn tài khoản của nạn nhân hoặc lừa họ xóa toàn bộ tài khoản Facebook của họ đòi hỏi thêm một số nỗ lực từ phía kẻ tấn công, vì nạn nhân cần nhập mật khẩu trước khi tài khoản bị xóa.

Để làm điều này, nhà nghiên cứu cho biết hacker sẽ yêu cầu các nạn nhân truy cập hai URL riêng biệt, một để thêm email hoặc số điện thoại và thực hiện xác thực.

Đó là "bởi vì các điểm cuối 'bình thường' được sử dụng để thêm email hoặc số điện thoại không có tham số 'tiếp theo' để chuyển hướng người dùng sau khi yêu cầu thành công", nhà nghiên cứu nói.

Tuy nhiên, nhà nghiên cứu vẫn chiếm toàn quyền với một URL bằng cách tìm các điểm cuối có tham số 'tiếp theo' và ủy quyền cho một ứng dụng độc hại thay cho nạn nhân và lấy mã thông báo truy cập Facebook của họ.

Với quyền truy cập vào mã thông báo xác thực của nạn nhân, khai thác sẽ tự động thêm địa chỉ email do kẻ tấn công kiểm soát vào tài khoản của họ, cho phép chiếm đoạt hoàn toàn tài khoản bằng cách đặt lại mật khẩu và khóa người dùng hợp pháp khỏi tài khoản Facebook.

Mặc dù vụ việc chiếm đoạt tài khoản Facebook không đơn giản, nhưng nhà nghiên cứu cho biết hacker cũng có thể chiếm đoạt tài khoản Facebook của bạn "trong chớp mắt".

Các cuộc tấn công chiếm đoạt tài khoản như vậy sẽ bị hạn chế phần nào nếu bạn đã bật xác thực hai yếu tố cho tài khoản Facebook của mình, ngăn chặn tin tặc đăng nhập vào tài khoản của bạn cho đến khi chúng xác minh mật mã 6 chữ số được gửi đến thiết bị di động của bạn.

Tuy nhiên, bất kỳ sự phòng chống nào cũng không thể ngăn chặn tin tặc lợi dụng lỗ hổng này, như thay đổi hoặc xóa ảnh hoặc album hồ sơ của bạn hoặc đăng bất cứ điều gì trên dòng thời gian của bạn.

Samm0uda đã báo cáo lỗ hổng này cho Facebook vào ngày 26 tháng 1. Facebook đã thừa nhận vấn đề này và giải quyết nó vào ngày 31 tháng 1, thưởng cho nhà nghiên cứu 25.000 USD.

Khuyến nghị:

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

Link tham khảo: https://whitehat.vn/threads/hacker-su-dung-link-doc-khai-thac-loi-tren-facebook.11990/

3. Lỗ hổng WinRAR ảnh hưởng đến tất cả các phiên bản phát hành trong 19 năm

Các nhà nghiên cứu về an ninh mạng đã tiết lộ chi tiết kỹ thuật về lỗ hổng nghiêm trọng trong WinRAR – một ứng dụng nén/giải nén tệp tin Windows phổ biến với 500 triệu người dùng trên toàn thế giới, lỗ hổng này ảnh hưởng đến tất cả các phiên bản phần mềm được phát hành trong 19 năm qua.

Lỗ hổng nằm trong một thư viện của bên thứ ba đã bị lỗi thời, được gọi là UNACEV2.DLL, thư viện này được sử dụng để xử lý trích xuất các tệp được nén ở định dạng ACE.

Tuy nhiên, vì WinRAR phát hiện định dạng theo nội dung của tệp chứ không dựa trên phần mở rộng cho nên kẻ tấn công có thể thay đổi phần mở rộng .ace thành phần mở rộng .rar để làm cho nó trông giống như bình thường.

Cách thức tấn công

Lỗi "Absolute Path Traversal" đã được tìm thấy trong thư viện được cho là điểm mấu chốt để các tin tặc có thể thực thi mã tùy ý trên một hệ thống được nhắm mục tiêu. Việc này cho phép giải nén một tệp tin nén lưu trữ các phần mềm độc hại sử dụng các phiên bản phần mềm có tồn tại lỗ hổng.

Lỗ hổng Path Traversal cho phép kẻ tấn công giải nén các tệp nén vào thư mục mà chúng chọn thay vì thư mục do người dùng chọn, tạo ra cơ hội lây nhiễm mã độc vào thư mục Windows Startup – nơi sẽ tự động chạy trong lần khởi động lại tiếp theo. Như được trình bày trong video, để kiểm soát hoàn toàn các máy tính được nhắm mục tiêu, tất cả những gì kẻ tấn công cần làm là thuyết phục người dùng mở tệp tin nén độc hại được tạo thủ công bằng WinRAR.

Do đội ngũ WinRAR đã mất mã nguồn của thư viện UNACEV2.dll vào năm 2005, nên giờ đây họ đã quyết định loại bỏ luôn UNACEV2.dll khỏi gói cung cấp để khắc phục sự cố và phát hành phiên bản WINRar 5.70 beta 1 không hỗ trợ định dạng ACE.

Tuy nhiên, để tránh bị tấn công, người dùng Windows nên cài đặt phiên bản WinRAR mới nhất càng sớm càng tốt và tránh mở các tệp tin nén được nhận được từ các nguồn không xác định.

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-anh-huong-den-tat-ca-cac-phien-ban-phat-hanh-trong-19-nam/

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	phpMyAdmin	CVE-2019-6798 CVE-2019-6799 …	Nhóm 02 lỗ hổng trên gói phần mềm nguồn mở phpMyAdmin (công cụ mà quản trị viên thường sử dụng để thao tác và quản lý cơ sở dữ liệu MySQL) phiên bản trước 4.8.5 cho phép đối tượng tấn công khai thác lỗi SQL Injection, truy cập và đọc bất kỳ tập tin nào trên máy chủ web.	Đã có thông tin xác nhận và bản vá
2	Adobe	CVE-2018-19721 CVE-2018-19723 CVE-2018-19724 ...	Nhóm 06 lỗ hổng trên một số sản phẩm, ứng dụng của Adobe (Adobe Acrobat & Reader; Adobe Experience Manager Forms) cho phép đối tượng tấn công thực hiện thu thập thông tin, chèn các đoạn mã độc hại để ăn trộm thông tin xác thực vfa chuyển hướng người dùng tới trang web độc hại	Đã có thông tin xác nhận và bản vá
3	Openssh	CVE-2019-6111 CVE-2019-6110	Nhóm 02 lỗ hổng trên phần mềm OpenSSH phiên bản 7.9 cho phép đối tượng tấn công ghi đè lên các tập tin bao gồm cả những tập tin xác thực của SSH như .ssh/authorized_keys khi thực hiện copy dữ liệu sử dụng SCP Ảnh hưởng tới tất cả thiết bị có cài đặt OpenSSH phiên bản 7.9	Đã có thông tin xác thực và bản vá Đã có mã khai thác
4	Debian -apt	CVE-2019-3462	Lỗ hổng trong phương thức giao dịch HTTP của gói ứng dụng APT cho phép đối tượng tấn công thực hiện tấn công nghe lén, thực thi mã lệnh.	Đã có thông tin xác nhận và bản vá

			Ảnh hưởng tới hệ điều hành debian và trên nền Debian như (Ubuntu) phiên bản 1.4.8 và phiên bản trước đó.	
5	D-link	CVE-2018-15516 CVE-2019-7297 CVE-2018-15515	Nhóm 05 lỗ hổng trên một số sản phẩm của D-Link (Central WiFiManage, D-Link DIR-823G) cho phép đối tượng tấn công thực hiện khai thác lỗi SSRF, tấn công leo thang chiếm quyền điều khiển thiết bị, chèn và thực thi lệnh của hệ điều hành.	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	disorderstatus.ru
2	differentia.ru
3	atomictrivia.ru
4	n39k7evp.ru
5	xjpakmdcfuqe.com
6	mv4j1vv1.ru
7	kukutrustnet777.info
8	plpanaifheaighai.com
9	n.hmiblgoja.ru
10	sz95sv2b.ru

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.