BẢN TIN NỘI BỘ

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

1. PuTTY phát hành bản cập nhật vá 8 lỗi nghiêm trọng mức cao

PuTTY là một trong những chương trình SSH Client mã nguồn mở phổ biến nhất và được sử dụng rộng rãi, cho phép người dùng truy cập máy tính từ xa qua các giao thức mạng SSH, Telnet và Rlogin.

Gần 20 tháng sau khi đưa ra phiên bản phần mềm trước đó, đầu tuần này các nhà phát triển của PuTTY đã phát hành phiên bản mới nhất 0.71 cho các hệ điều hành Windows và Unix.

Theo khuyến cáo của hãng, tất cả các phiên bản trước của phần mềm PuTTY được cho là có nhiều lỗ hổng an ninh, có thể cho phép máy chủ độc hại hoặc máy chủ bị xâm nhập chiếm quyền điều khiển hệ thống của khách hàng theo những cách khác nhau.

Sau đây là danh sách 8 lỗ hổng được PuTTY 0.71 vá:

1. Giả mạo nhắc nhở xác thực - Vì PuTTY không có cách để xác định thiết bị đầu cuối có đáng tin hay không, do vậy giao diện người dùng có thể bị máy chủ độc hại khai thác để tạo một nhắc nhở xác thực giả ở phía máy khách, lừa nạn nhân nhập mật khẩu.

2. Thực thi mã thông qua hình thức tấn công độc hại CHM Hijacking - Khi người dùng khởi chạy trợ giúp trực tuyến trong các công cụ GUI PuTTY, phần mềm sẽ cố gắng xác định vị trí tệp trợ giúp cùng với tệp thực thi của chính nó.

Hành vi này có thể cho phép kẻ tấn công lừa người dùng thực thi mã độc trên hệ thống máy khách thông qua tệp CHM.

3. Lỗi tràn bộ đệm trong các Công cụ PuTTY Unix - Theo khuyến cáo, nếu một máy chủ mở quá nhiều lệnh chuyển tiếp cổng, PuTTY trên Unix sẽ không kiểm tra đặc tả tệp tin đầu vào (file descriptor) mà nó thu thập trong quá trình giám sát các tệp Unix đang hoạt động, dẫn đến lỗi tràn bộ đệm.

"Chúng tôi không biết lỗi này có thể bị khai thác từ xa hay không, nhưng ít nhất nó có thể được kích hoạt từ xa bởi một máy chủ SSH độc hại, nếu bạn bật bất kỳ tùy chọn nào cho phép máy chủ mở kênh: chuyển tiếp cổng từ xa sang cục bộ, chuyển tiếp chủ động hoặc chuyển tiếp X11", khuyến cáo cho hay.

4. Sử dụng lại số ngẫu nhiên mã hóa - Vấn đề này nằm ở trình tạo số ngẫu nhiên mã hóa trong PuTTY, trình này đôi khi sử dụng cùng một lô byte ngẫu nhiên hai lần.

"Sự việc này xảy ra do lỗi tràn bộ đệm một byte trong mã nhóm ngẫu nhiên. Nếu entropy từ nguồn bên ngoài được đưa vào nhóm ngẫu nhiên khi chỉ mục vị trí hiện tại đang chỉ vào cuối nhóm đó, nó sẽ tràn qua bộ đệm nhóm một byte và ghi đè lên chỗ byte thấp của chính chỉ mục vị trí đó".

5. Lỗ hổng tràn số nguyên - Tất cả các phiên bản trước của PuTTY đều gặp phải sự cố tràn số nguyên do thiếu trao đổi khóa RSA kiểm tra kích thước khóa.

Một máy chủ từ xa có thể kích hoạt lỗ hổng bằng cách gửi khóa RSA ngắn, dẫn đến tràn số nguyên và ghi đè bộ nhớ không kiểm soát được.

Các nhà phát triển PuTTY không chắc chắn liệu lỗ hổng này có thể bị khai thác để giành quyền kiểm soát máy khách hay không, nhưng vì sự cố xảy ra trong quá trình trao đổi khóa và xảy ra trước khi kiểm tra khóa máy chủ, sự cố tràn có thể xảy ra do tấn công MitM ngay cả khi người trung gian không biết khóa máy chủ chính xác.

Vì vậy, ngay cả khi bạn tin tưởng máy chủ bạn đang kết nối, bạn vẫn không an toàn.

6, 7 và 8. Tấn công DoS thiết bị đầu cuối - Ba lỗ hổng cuối cùng trong PuTTY khiến máy chủ crash hoặc làm chậm thiết bị đầu cuối của khách hàng bằng cách gửi các đầu ra văn bản khác nhau.

Máy chủ có thể gửi một chuỗi ký tự Unicode dài không bị gián đoạn đến thiết bị đầu cuối của máy khách, điều này có thể dẫn đến một cuộc tấn công từ chối dịch vụ bằng cách khiến hệ thống phân bổ số lượng bộ nhớ không giới hạn.

Cuộc tấn công DoS thứ hai có thể được kích hoạt bằng cách gửi các ký tự kết hợp, có độ rộng gấp đôi, số lượng cột đầu cuối lẻ và toolkit GTK đến output của máy khách.

Trong cuộc tấn công DoS thứ ba, bằng cách gửi các ký tự có độ rộng gấp 2 được sử dụng bởi người Trung Quốc, Nhật Bản và Hàn Quốc cho khách hàng, trình giả lập thiết bị đầu cuối của PuTTY có thể bị buộc crash.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng và người quản trị cần cập nhật phiên bản mới nhất của phần mềm Putty (nếu đang sử dụng) để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/putty-phat-hanh-ban-cap-nhat-va-8-loi-nghiem-trong-muc-cao.12080/

2. Libssh phát hành bản cập nhật vá 9 lỗ hổng an ninh mới

Libssh2, một thư viện mã nguồn mở phổ biến, vừa phát hành phiên bản mới nhất để vá tổng cộng 9 lỗ hổng an ninh có thể dẫn đến chiếm quyền điều khiển từ xa.

Thư viện Libssh2 được tất cả các nhà phân phối lớn của hệ điều hành Linux hỗ trợ, bao gồm Ubuntu, Red Hat, Debian...

Tất cả lỗ hổng được vá trong libssh2 phiên bản 1.8.1 đều dẫn đến lỗi bộ nhớ, từ đó gây ra thực thi mã tùy ý trong một số trường hợp nhất định.

Một số lỗ hổng nghiêm trọng được vá trong Libssh:

Lỗi tràn số nguyên CVE-2019-3855, CVE-2019-3856, CVE-2019-3857: Nếu một server ssh đã bị hacker chiếm quyền điều khiển và máy client cần ssh lên server có chứa lỗ hổng (cài libssh2 < 1.8.1), thì hacker có thể xâm nhập từ server ssh sang máy client.

Lỗi ghi dữ liệu ngoài vùng bộ nhớ (out-of-bounds write) CVE-2019-3858, CVE-2019-3859, CVE-2019-3860, CVE-2019-3862: Máy chủ SSH độc hại có thể gây ra lỗi DoS hoặc đọc được dữ liệu trên máy khách.

Các lỗ hổng này ảnh hưởng đến tất cả các phiên bản Libssh2 trước 1.8.1. Hiện chưa ghi nhận bất kỳ mã khai thác của các lỗ hổng này.

Nếu bạn đang sử dụng Libssh, hãy cài đặt bản cập nhật của Libssh càng sớm càng tốt. Với các phiên bản hệ điều hành Linux, người dùng nên nhanh chóng cập nhật hệ điều hành.

Đây không phải là lần đầu tiên thư viện phổ biến này được phát hiện tồn tại các vấn đề an ninh. Cuối năm ngoái, các nhà phát triển đã vá một lỗ hổng nghiêm trọng bốn năm tuổi trong Libssh, cho phép kẻ tấn công chiếm quyền kiểm soát máy chủ SSH mà không cần mật khẩu.

Khuyến nghị:

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

Link tham khảo: https://whitehat.vn/threads/libssh-phat-hanh-ban-cap-nhat-va-9-lo-hong-an-ninh-moi.12073/

3. Biến thể Mirai thêm nhiều mã khai thác mới, nhắm vào thiết bị IoT doanh nghiệp

Các chuyên gia vừa phát hiện một biến thể mới trong mạng botnet IoT khét tiếng Mirai, lần này nhắm mục tiêu tới các thiết bị sử dụng trong doanh nghiệp. Mã độc tăng cường kiểm soát băng thông lớn hơn để thực hiện các cuộc tấn công DDoS phá hoại.

Mặc dù những kẻ ban đầu tạo ra botnet Mirai đã bị bắt và bỏ tù, các biến thể của mã độc IoT khét tiếng này, bao gồm Satori và Okiru, vẫn tiếp tục xuất hiện do có sẵn mã nguồn trên Internet kể từ 2016.

Xuất hiện lần đầu năm 2016, Mirai được biết đến là mã độc botnet IoT có khả năng lây nhiễm router (bộ định tuyến), camera an ninh, đầu ghi hình DVR và các thiết bị thông minh khác – vốn thường sử dụng thông tin đăng nhập mặc định và chạy các phiên bản lỗi thời của Linux. Từ các thiết bị này, một botnet được tạo thành để tiến hành các cuộc tấn công DDoS.

Biến thể Mirai mới nhắm tới các thiết bị IoT doanh nghiệp

Các chuyên gia Palo Alto Network Unit 42 phát hiện biến thể mới nhất của Mirai lần đầu tiên nhắm mục tiêu vào các thiết bị doanh nghiệp, bao gồm các hệ thống Thuyết trình không dây WePftime WiPG-1000 và các TV LG Supersign.

Biến thể Mirai bổ sung thêm 11 mã khai thác mới, nâng tổng số lên 27, cùng với bộ "thông tin mặc định" mới để sử dụng trong các cuộc tấn công dò tìm mật khẩu nhắm vào các thiết bị kết nối Internet.

"Các tính năng mới này mang lại cho botnet một trường tấn công lớn. Đặc biệt, việc nhắm mục tiêu vào các doanh nghiệp cũng cho phép quyền truy cập băng thông lớn hơn, cuối cùng dẫn đến hỏa lực mạnh hơn cho botnet để tấn công DDoS", các chuyên gia cho biết.

Trong khi mã khai thác thực thi từ xa đối với TV LG Supersign (CVE-2018-17173) đã xuất hiện từ tháng 9 năm ngoái, đoạn mã khai thác lỗ hổng trong WePftime WiPG-1000 được công khai từ năm 2017.

Ngoài hai mã khai thác này, biến thể Mirai mới cũng đang nhắm mục tiêu vào nhiều thiết bị phần cứng như:

Router Linksys

Router ZTE

Router DLink

Thiết bị lưu trữ mạng

Đầu ghi hình NVR và camera IP

Sau khi quét và xác định các thiết bị dễ bị tấn công, mã độc sẽ lấy bộ tải Mirai mới từ một trang web bị xâm nhập và tải xuống thiết bị đích, sau đó thêm thiết bị vào mạng botnet và cuối cùng sử dụng để khởi chạy các cuộc tấn công HTTP Flood DDoS.

Mirai là mạng botnet khét tiếng chịu trách nhiệm cho một số vụ tấn công DDoS kỷ lục, bao gồm cả các cuộc tấn công nhắm vào nhà cung cấp dịch vụ lưu trữ OVH và Dyn DNS có trụ sở tại Pháp, làm tê liệt một số trang web lớn nhất thế giới, bao gồm Twitter, Netflix, Amazon và Spotify.

Các cuộc tấn công dựa trên Mirai gia tăng đột ngột sau khi mã nguồn được công bố vào tháng 10/2016, cho phép kẻ tấn công nâng cấp mã độc với các mã khai thác mới tùy theo nhu cầu và mục tiêu.

Các chuyên gia cho biết: “Những phát triển [mới] này càng khẳng định tầm quan trọng việc các doanh nghiệp quan tâm hơn tới các thiết bị IoT trên mạng của mình, thay đổi mật khẩu mặc định, đảm bảo rằng các thiết bị được cập nhật đầy đủ các bản vá”.

“Và trong trường hợp các thiết bị không thể vá được, hãy loại bỏ các thiết bị đó khỏi mạng như phương sách cuối cùng”.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần thay đổi mật khẩu mặc định cho các thiết bị được kết nối internet ngay khi mang chúng về nhà hoặc văn phòng và luôn cập nhật đầy đủ các bản vá mới nhất để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/bien-the-mirai-them-nhieu-ma-khai-thac-moi-nham-vao-thiet-bi-iot-doanh-nghiep.12072/

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	Cisco	CVE-2019-1601 CVE-2019-1615 CVE-2019-1723 ...	Nhóm 22 lỗ hổng trên một số sản phẩm của Cisco (NX-OS Software, FXOS Software, Small Business SPA500 Series IP Phones, Enterprise Chat and Email, DNA Center ...) gồm: lỗ hổng trong việc phân quyền tập tin cho phép truy cập và sửa đổi trái phép tập tin cấu hình quan trọng của hệ thống, lỗ hổng XSS, và nhiều lỗ hổng trong các thành phần khác nhau của Cisco NX-OS cho phép chèn và thực thi mã lệnh trái phép.	Đã có thông tin xác nhận và bản vá
2	F5	CVE-2019-6597 CVE-2019-6598 CVE-2019-6599 ...	Nhóm 06 lỗ hổng trên các sản phẩm BIG-IP và Enterprise Manager của F5 cho phép đối tượng tấn công khai thác lỗi XSS để ăn trộm thông tin xác thực, thực thi đoạn mã độc hại thông qua lỗi trong việc xử lý file ảnh và file PDF.	Đã có thông tin xác nhận và bản vá
3	Google Android	CVE-2019-9833 CVE-2019-9832	Nhóm 02 lỗi trong một số ứng dụng mặc định của Android (Screen Stream, Airdrop) cho phép thực hiện tấn công từ chối dịch vụ từ xa.	Đã có thông tin xác nhận và bản vá. Đã có mã khai thác
4	IBM	...	Nhóm 31 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	Đã có thông tin xác nhận và bản vá.

			bộ đệm để chèn và thực thi mã lệnh, tấn công leo thang.	
5	Joomla	CVE-2019-9711 CVE-2019-9712 CVE-2019-9713 ...	Nhóm 04 lỗ hổng trên một số phiên bản của phần mềm nguồn mở Joomla cho phép khai thác lỗi XSS để ăn trộm thông tin xác thực và thực hiện những tấn công sâu hơn.	Đã có thông tin xác nhận và bản vá
6	Rdesktop	CVE-2018-20180 CVE-2018-20181 CVE-2018-20182 ...	Nhóm 09 lỗ hổng trong phần mềm Rdesktop (phần mềm Remote Desktop thường sử dụng trên các hệ điều hành Linux) cho phép khai thác nhiều lỗi khác nhau trong đó có nhiều lỗi tràn bộ đệm để chèn và thực thi mã lệnh. Ảnh hưởng tới các phiên bản Rdesktop 1.8.3 và các phiên bản trước đó; FreeRDP phiên bản 2.0.0-rc4 và các phiên bản trước đó.	Đã có thông tin xác nhận và bản vá
7	Intel	CVE-2019-0129 CVE-2018-12185 CVE-2018-12221 ...	Nhóm 40 lỗ hổng trên một số sản phẩm, ứng dụng của Intel (Intel(R) AMT, CSME, Intel(R) Graphics Driver, Intel(R) USB 3.0 Creator Utility, Active Management Technology,) cho phép đối tượng tấn công thực thi mã lệnh qua các giao tiếp vật lý, tấn công leo thang, tấn công từ chối dịch vụ.	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	soplifan.ru
6	ep08tzvn7.ru
7	xjpakmdcfuqe.com

8	somicrososoft.ru
9	00o9jtv2.ru
10	morphed.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.