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

1. Công an Hà Nội cảnh báo về mã độc ngụy trang tài liệu về virus corona

Công an TP. Hà Nội mới đây vừa phát đi cảnh báo về việc mã độc ngụy trang dưới tập tin có nội dung liên quan đến virus corona.

Cụ thể, qua công tác nắm tình hình, các đơn vị nghiệp vụ công an TP. Hà Nội phát hiện hành vi phát tán mã độc ẩn dưới các tập tài liệu liên quan đến virus Covid-19. Các mã độc này cho phép hacker làm hư hại, chỉnh sửa hoặc sao chép dữ liệu, thậm chí can thiệp vào hoạt động của máy tính hoặc mạng máy tính của người dùng.

Các chuyên gia nghiên cứu mã độc của Kaspersky dự đoán số lượng mã độc được phát tán dựa trên thông tin về virus corona sẽ ngày càng tăng cao do thông tin về dịch bệnh COVID-19 hay corona đang là chủ đề nóng được nhiều người quan tâm.

Các đối tượng sẽ sử dụng thông tin này như mồi nhử để thực hiện các hành vi phạm tội, phát tán mã độc dưới dạng tên:
Worm.VBS.Dinihou.r; Worm.Python.Agent.;UDS:DangerousObject.Multi.Generic; Trojan.WinLNK.Agent.gg;Trojan.WinLNK.Agent.ew; HEUR:Trojan.PDF.Badur.b; HEUR:Trojan.WinLNK.Agent.gen.

Để tránh trở thành nạn nhân của mã độc này, Công an TP. Hà Nội đã khuyến cáo người dân tránh truy cập các liên kết nghi vấn liên quan tới virus corona, trừ những thông tin được đăng tải bởi các cơ quan chính thống và từ những nguồn tin đáng tin cậy.

Khi nhận được tập tin đính kèm, người dùng cần chú ý phần mở rộng của tập tin tải xuống, cẩn thận với những tài liệu và tệp video có định dạng ".exe" hoặc ".lnk".

Bên cạnh đó, người dùng cũng nên chủ động trang bị những giải pháp bảo mật, cài đặt phần mềm diệt virus để tránh những mối đe dọa từ mã độc, nâng cao khả năng bảo vệ hệ thống thông tin trên mạng.

Khuyến nghị: Người dùng cần tuân thủ các quy định đã ban hành, không nhấn vào các đường link lạ để đảm bảo an toàn thông tin.

Link tham khảo: http://antoanthongtin.vn/an-toan-thong-tin/cong-an-ha-noi-canh-bao-ve-ma-doc-nguy-trang-tai-lieu-ve-virus-corona-105863

2. Google cấm cửa 600 ứng dụng "khủng bố" người dùng bằng quảng cáo

Tổng cộng 600 ứng dụng trên Google Play Store đã bị gỡ bỏ và cấm cửa qua cơ chế Google AdMob và Google Ad Manager sau khi bị phát hiện liên tục "bỏ bom" người dùng bằng quảng cáo phiền nhiễu.

Hành động này vi phạm chính sách của Google, đại diện của công ty giải thích. Vị này cho biết gian dối quảng cáo di động cũng là vấn đề mà công ty đang đối phó nghiêm túc.

"Tại Google, chúng tôi có đội nhóm riêng giúp phát hiện và ngăn chặn các nhà phát triển ác ý có ý định qua mặt hệ sinh thái di động. Là một phần của nỗ lực này, nhiều ứng dụng đã bị gỡ bỏ do vi phạm chính sách", Per Bjorke, giám đốc sản phẩm cao cấp phụ trách bộ phận Ad Traffic Quality của Google, cho biết.

Tuy Google không công bố tên ứng dụng bị gỡ bỏ khỏi Google Play Store, công ty này đã cảnh cáo các nhà phát triển "nhúng chàm".

Thực tế, ứng dụng ác ý trên Google Play Store không phải chủ đề mới mẻ. Các nhà nghiên cứu bảo mật luôn khuyến nghị người dùng cần đọc kỹ thông tin về ứng dụng trước khi tải xuống.

Một trong những cách tìm hiểu tốt nhất là đọc bình luận về ứng dụng. Tại đó, người dùng chia sẻ về các vấn đề gặp phải khi họ trải nghiệm ứng dụng.

Khuyến nghị: Người dùng cần kiểm tra kỹ thông tin trước khi cài đặt những ứng dụng mới để đảm bảo an toàn thông tin.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/google-cam-cua-600-ung-dung-android-do-khung-bo-nguoi-dung-bang-quang-cao-618850.html

3. Lỗ hổng tấn công từ xa nghiêm trọng trên Trình quản lý bản quyền phần mềm của Cisco

Mật khẩu mặc định cho phép tất cả mọi người truy cập vào Smart Software Manager On-Prem Base (SSM On-Prem Base - Trình quản lý phần mềm thông minh trên nền tảng lưu trữ dữ liệu tại chỗ) của Cisco mà không cần nền tảng này phải kết nối Internet.

Một lỗ hổng nghiêm trọng trong dịch vụ High Availability của nền tảng Smart Software Manager On-Prem Base đã được phát hiện. Lỗ hổng cho phép hacker tấn công từ xa bằng cách sử dụng mật khẩu mặc định.

SSM On-Prem Base của Cisco được sử dụng để quản lý bản quyền sản phẩm của khách hàng hoặc đối tác, cung cấp khả năng hiển thị và báo cáo sát theo thời gian thực được hãng này mua và sử dụng. Cisco cho biết nền tảng này hướng đến các khách hàng có nhu cầu bảo mật nghiêm ngặt và không muốn sản phẩm của họ giao tiếp với cơ sở dữ liệu cấp phép trung tâm trên SSM qua kết nối Internet trực tiếp, như các tổ chức tài chính, nhà cung cấp dịch vụ và các tổ chức chính phủ.

Theo thông báo của Cisco, mật khẩu được mã hóa cứng dành cho tài khoản hệ thống [HA] không thuộc quyền kiểm soát của quản trị viên hệ thống. Về cơ bản, bất kỳ ai phát hiện ra mật khẩu (có thể trong hướng dẫn cài đặt hoặc tài liệu khác có sẵn trực tuyến), đều có thể đăng nhập vào tài khoản này và sau đó, kết nối với SSM On-Prem Base của Cisco.

Chuyên gia và là giám đốc an ninh thông tin tại Automox cho biết, lỗ hổng trên rất dễ dàng bị khai thác: "Các hệ thống có thông tin đăng nhập mã hóa cứng mặc định hoàn toàn không cần bất kỳ kỹ năng chuyên môn nào và không hề mất thời gian để tấn công".

Lỗ hổng, có điểm CVSS là 9,8, "có thể cho phép kẻ tấn công từ xa không cần xác thực truy cập vào một phần nhạy cảm của hệ thống bằng tài khoản có đặc quyền cao. Khai thác thành công, kẻ tấn công có thể truy cập để đọc và ghi vào dữ liệu hệ thống, bao gồm cả cấu hình của thiết bị".

May mắn là kẻ tấn công sẽ không đủ quyền quản trị để kiểm soát thiết bị.

Dù chưa xử lý vấn đề triệt để nhưng Cisco đã phát hành một bản vá cho lỗi này (Cisco Smart Software Manager On-Prem 7-202001). Lỗ hổng chỉ ảnh hưởng đến các hệ thống nếu tính năng HA được kích hoạt (HA không được bật mặc định).

Khuyến nghị: Người quản trị cần tuân thủ các quy định đã ban hành về việc sự dụng mật khẩu an toàn và cập nhật bản vá mới nhất của sản phẩm Cisco để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/lo-hong-tan-cong-tu-xa-nghiem-trong-tren-trinh-quan-ly-ban-quyen-phan-mem-cua-cisco.13246/

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	Wordpress	CVE 2013 2010 CVE 2013 3684 CVE 2014 8739 …	Nhóm 14 lỗ hổng trên phần mềm Wordpress (Wordpress W3 Total Cache Plugin, NextGEN Gallery plugin,...) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, tấn công XSS, tấn công CSRF.	Đã có thông tin xác nhận và bản vá.
2	Chrome	CVE 2020 6406 CVE 2020 6414 CVE 2020 6392 …	Nhóm 36 lỗ hổng trên Chrome (Safe Browsing in Google Chrome, Blink in Google Chrome…) cho phép đối tượng tấn công chèn và thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá
3	Cisco	CVE 2020 3111 CVE 2020 3110 CVE 2013 2683 …	Nhóm 02 lỗ hổng trên sản phẩm của Cisco (Cisco ACE A2(3.6), Cisco IOS…) cho phép đối tượng tấn công tấn công tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
4	Adobe	CVE 2020 3740 CVE 2020 3733 CVE 2020 3731 …	Nhóm 42 lỗ hổng trên phần mềm Adobe (Adobe Framemaker versions 2019.0.4,…) cho phép đối tượng tấn công chèn và thực thi mã tùy ý. 01 lỗ hổng có điểm CVSS: 10.0 (đặc biệt nghiêm trọng).	Đã có thông tin xác nhận và bản vá
5	D link	CVE 2013 5945 CVE 2020 8962 CVE 2013 3096	Nhóm 03 lỗ hổng trên sản phẩm của D-link (DSR 150, DIR865L v1.03,…) cho phép đối tượng tấn công chèn và thực thi mã tùy ý. 01 lỗ hổng có điểm CVSS: 10.0 (đặc biệt nghiêm trọng).	Đã có thông tin xác nhận và bản vá
6	Microsoft	CVE 2020 7978 CVE 2020 7966 CVE 2020 7968 …	Nhóm 99 lỗ hổng trên một số sản phẩm của Microsoft (ChakraCore, Internet Explorer, Excel software,…)	Đã có thông tin xác nhận và bản vá

			cho phép đối tượng tấn công chèn và thực thi mã tùy ý.	
7	Linux	CVE 2009 4067 CVE 2012 0810 CVE 2020 8992 …	Nhóm 03 lỗ hổng trên hệ điều hành Linux (Linux kernel,…) cho phép đối tượng tấn công 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	ydbnsrt.me
5	iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
6	xdqzpbcgrvkj.ru
7	somicrososoft.ru
8	cp.qrkqnyr0.ru
9	www.cityofangelsmagazine.com
10	soplifan.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.