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

1. Bộ TT&TT cấp Giấy phép cung cấp dịch vụ chứng thực chữ ký số công cộng cho nhà cung cấp thứ 15

Ngày 28/2, Công ty cổ phần đầu tư công nghệ và thương mại Softdreams đã được Bộ Thông tin và Truyền thông cấp giấy phép cung cấp dịch vụ chứng thực chữ ký số công cộng và trở thành đơn vị thứ 15 cung cấp dịch vụ tại Việt Nam.

Theo thông tin từ Trung tâm Chứng thực điện tử quốc gia, Giấy phép cung cấp dịch vụ chứng thực chữ ký số công cộng với tên giao dịch EasyCA được Bộ trưởng Bộ TT&TT ký ngày 21/2/2020 và có giá trị đến hết ngày 20/2/2030.

Đại diện Trung tâm Chứng thực điện tử quốc gia cho biết, sau khi nhận được đơn kèm hồ sơ đề nghị cấp phép của Công ty cổ phần đầu tư công nghệ Softdreams, Trung tâm Chứng thực quốc gia đã phối hợp với Ban Cơ yếu Chính phủ và 6 đơn vị thuộc Bộ TT&TT, các đơn vị chuyên trách của Bộ Công an để thẩm tra. Công ty cổ phần đầu tư công nghệ Softdreams đã đạt được đầy đủ những điều kiện để cấp phép trở thành nhà cung cấp dịch vụ chứng thực chữ ký số công cộng tiêu chuẩn.

Theo Giấy phép, Công ty cổ phần đầu tư công nghệ Softdreams được cung cấp dịch vụ chứng thực chữ ký số với 3 loại chứng thư: Chứng thư số cho cá nhân, tổ chức; Chứng thư số SSL dành cho máy chủ; Chứng thư số cho phần mềm và phương thức lưu khóa bí mật của thuê bao. Theo đó tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng EASYCA lưu khóa bí mất của thuê bao trong USB Token đáp ứng tiêu chuẩn FIPS PUB 140 – 2 tối thiểu mức 2.

Đại diện công ty cho biết, hiện tại, công ty đang cung cấp dịch vụ hóa đơn điện tử cho gần 40.000 khách hàng là tổ chức, doanh nghiệp và phần mềm kế toán cho khoảng 15.000 doanh nghiệp. Đại diện công ty này cũng cho biết đang cung cấp giải pháp cho Cổng thông tin tín dụng quốc gia Việt Nam.

Link tham khảo: http://antoanthongtin.vn/ca-cong-cong/bo-tttt-cap-giay-phep-cung-cap-dich-vu-chung-thuc-chu-ky-so-cong-cong-cho-nha-cung-cap-thu-15-105889

2. Lỗ hổng bảo mật Apache Tomcat chiếm quyền điều khiển máy chủ

VSEC vừa phát đi cảnh báo về Ghostcat - một lỗ hổng rủi ro cao trên phần mềm mã nguồn mở Apache Tomcat có thể ảnh hưởng tới hơn 1 triệu máy chủ đang hoạt động trên thế giới, trong đó có Việt Nam.

Lỗ hổng cho phép kẻ tấn công có thể đọc các tệp tin cấu hình của ứng dụng, đánh cắp mật khẩu hoặc API token, thậm chí chiếm quyền điều khiển máy chủ.

Ghostcat là một lỗ hổng trong giao thức AJP Tomcat (Apache JServ Protocol) Apache Tomcat - là phần mềm web server mã nguồn mở miễn phí, được sử dụng để chạy các ứng dụng web lập trình bằng ngôn ngữ java.

Tuy là phần mềm miễn phí, nhưng Apache Tomcat được đánh giá cao bởi khả năng thiết lập môi trường website an toàn, tiết kiệm chi phí và tính hiệu quả cao. Đó cũng là lý do mà Apache Tomcat luôn nằm trong danh sách những phần mềm mã

nguồn mở phổ biến nhất hiện nay trên thế giới và được sử dụng rộng rãi bởi nhiều đơn vị trong lĩnh vực tài chính, ngân hàng, viễn thông... Do đó, việc xuất hiện lỗ hổng trên phần mềm này được đánh giá là cực kỳ nguy hiểm.

Lỗ hổng Ghostcat được theo dõi với mã CVE-2020-1938 (CVSS 9.8), được tin tặc khai thác dưới dạng chèn ký tự đặc biệt trong lúc gửi những yêu cầu tới máy chủ để đọc mã nguồn hoặc các thông tin file cấu hình máy chủ. Khi nắm được các file cấu hình này, tin tặc có thể tiếp cận và cài đặt backdoor (cửa hậu) để chiếm quyền điều khiển từ xa và thực thi các cuộc tấn công mạng khác.

Theo các chuyên gia Công ty cổ phần An ninh mạng VSEC, lỗ hổng Ghostcat hiện đã được phát hiện trên tất cả phiên bản (9.x/8.x/7.x/6.x) của Apache Tomcat phát hành trong suốt 13 năm qua, và điều đặc biệt nghiêm trọng là các mã khai thác đã xuất hiện và được chia sẻ tràn lan trên internet, từ đó các tin tặc có thể tìm kiếm và triển khai các phương thức xâm nhập vào máy chủ web một cách dễ dàng.

Theo công cụ tìm kiếm lỗ hổng BinaryEdge, hiện nay có hơn một triệu máy chủ Tomcat đang hoạt động, do đó các chuyên gia VSEC nhấn mạnh tất cả doanh nghiệp, cá nhân sử dụng Apache Tomcat mà không cập nhật lên phiên bản mới nhất đều nằm trong danh sách có thể trở thành con mồi của kẻ tấn công.

Vì vậy, VSEC khuyến cáo nếu các doanh nghiệp sử dụng hệ thống Apache Tomcat hãy cập nhật hệ thống lên phiên bản mới nhất, không mở cổng AJP đến các máy Client không đáng tin cậy.

Khuyến nghị: Người quản trị sử dụng hệ thống Apache Tomcat hãy cập nhật hệ thống lên phiên bản mới nhất, không mở cổng AJP đến các máy Client không đáng tin cậy để đảm bảo an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/lo-hong-bao-mat-apache-tomcat-chiem-quyen-dieu-khien-may-chu-1191551.html

3. Nhiều nhóm hacker đang tấn công máy chủ Microsoft Exchange

Các nhóm hacker được nhà nước bảo trợ đang khai thác lỗ hổng trong các máy chủ email Microsoft Exchange mà Microsoft đã vá trong Patch Tuesday tháng 2 năm 2020.

Các nỗ lực khai thác được phát hiện bởi công ty an ninh mạng Volexity của Anh vào thứ Sáu tuần trước. Tuy nhiên, Volexity không chia sẻ tên của các nhóm hacker đang khai thác lỗ hổng này.

Lỗ hổng trong Microsoft Exchange

Dưới đây là bản tóm tắt các chi tiết kỹ thuật của lỗ hổng (CVE-2020-0688):

• Trong quá trình cài đặt, máy chủ Microsoft Exchange không thể tạo khóa duy nhất cho mỗi phiên đăng nhập bảng điều khiển Exchange.

• Điều này có nghĩa là tất cả máy chủ email Microsoft Exchange được phát hành trong hơn 10 năm qua sử dụng các khóa giống hệt nhau (verifyKey và decryptKey) cho phần backend của bảng điều khiển.

• Kẻ tấn công có thể gửi các yêu cầu không đúng định dạng đến bảng điều khiển Exchange với dữ liệu serialized độc hại.

• Vì tin tặc biết các khóa mã hóa của bảng điều khiển, chúng có thể đảm bảo dữ liệu serialized được unserialized, dẫn đến mã độc chạy trên phần backend của máy chủ Exchange.

• Mã độc chạy với các đặc quyền hệ thống, cho phép kẻ tấn công toàn quyền kiểm soát máy chủ.

Microsoft đã phát hành bản vá cho lỗ hổng này vào ngày 11 tháng 2, khi đó hãng cũng cảnh báo các quản trị hệ thống cài đặt bản sửa lỗi càng sớm càng tốt, dự đoán các cuộc tấn công trong tương lai.

Không có gì xảy ra trong gần hai tuần sau đó. Tuy nhiên, mọi thứ đã leo thang vào cuối tháng, khi nhóm Zero-Day Initiative, đơn vị đã báo cáo lỗi này cho Microsoft, xuất bản một báo cáo kỹ thuật chi tiết lỗi và cách thức hoạt động của lỗ hổng.

Báo cáo được dùng như một hướng dẫn cho các nhà nghiên cứu an ninh tạo ra proof-of-concept để kiểm tra máy chủ của họ. Ít nhất ba trong số các PoC này đã được tìm thấy trên GitHub.

Cũng giống như trong nhiều trường hợp khác, một khi các chi tiết kỹ thuật và PoC được công khai, tin tặc cũng bắt đầu chú ý.

Vào ngày 26 tháng 2, một ngày sau khi báo cáo chi tiết về lỗ hổng được phát hành, các nhóm tin tặc bắt đầu rà quét Internet tìm kiếm các máy chủ Exchange. Các bản quét đầu tiên được phát hiện bởi công ty Bad Packets.

Và giờ, theo Volexity, các bản quét tìm kiếm máy chủ Exchange đã biến thành các cuộc tấn công thực tế.

Lỗ hổng đã được sử dụng trong các cuộc tấn công APT. Các nhà nghiên cứu cũng dự đoán rằng lỗi này sẽ trở nên phổ biến với các băng đảng ransomware thường xuyên nhắm vào các mạng doanh nghiệp.

Vũ khí hóa các thông tin đăng nhập "vô dụng" trước đó

Lỗ hổng Exchange này không dễ khai thác. Các chuyên gia không thấy lỗi này bị lạm dụng bởi các kiddies script (thuật ngữ được dùng để mô tả các tin tặc cấp thấp, không có kỹ năng).

Để khai thác lỗi Exchange CVE-2020-0688, tin tặc cần thông tin đăng nhập cho tài khoản email trên máy chủ Exchange - thứ mà các kiddies script thường không có.

Lỗ hổng CVE-2020-0688 là một lỗi được gọi là lỗi sau xác thực. Trước tiên, tin tặc cần đăng nhập và sau đó chạy payload độc hại chiếm quyền điều khiển máy chủ email của nạn nhân.

Với điều kiện hạn chế này, chỉ các nhóm APT và ransomware là có khả năng vì họ thường dành phần lớn thời gian để khởi động các chiến dịch lừa đảo, sau đó có được thông tin email nhân viên của công ty.

Nếu một tổ chức thực thi xác thực hai yếu tố (2FA) cho tài khoản email, những thông tin đó về cơ bản là vô dụng vì tin tặc không thể vượt qua 2FA.

Lỗi CVE-2020-0688 cho phép các APT tìm thấy mục đích cho các tài khoản cũ hơn được bảo vệ bởi 2FA mà họ đã chiếm đoạt được nhiều tháng hoặc nhiều năm trước đó.

Họ có thể sử dụng bất kỳ thông tin đăng nhập cũ nào như một phần để khai thác CVE-2020-0688 mà không cần phải vượt qua 2FA, nhưng vẫn chiếm quyền máy chủ Exchange của nạn nhân.

Do đó, các tổ chức được khuyến cáo cập nhật máy chủ email Exchange của họ với bản cập nhật bảo mật tháng 2 năm 2020 càng sớm càng tốt.

Tất cả các máy chủ Microsoft Exchange được coi là dễ bị tấn công, ngay cả các phiên bản đã kết thúc vòng đời (EoL). Đối với các phiên bản EoL, các tổ chức nên xem xét cập nhật lên phiên bản Exchange mới hơn. Nếu cập nhật máy chủ Exchange không phải là một tùy chọn, các công ty nên buộc thiết lập lại mật khẩu cho tất cả các tài khoản Exchange.

Trước đó, Cục An toàn thông tin đã cảnh báo nguy cơ tấn công mạng vào các máy chủ thư điện tử sử dụng Microsoft Exchange. Trong thông tin cảnh báo mới phát ra, Cục An toàn thông tin (Bộ TT&TT) đề nghị các cơ quan, đơn vị rà soát các máy chủ có cài đặt Microsoft để phát hiện và xử lý kịp thời các máy chủ có khả năng đã bị đối tượng tấn công khai thác qua lỗ hổng "CVE-2020-0688".

Khuyến nghị: Người quản trị cần cập nhật các bản vá mới nhất của Microsoft Exchange để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/nhieu-nhom-hacker-dang-tan-cong-may-chu-microsoft-exchange.13321/

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-2020-1938 CVE-2020-1937 CVE-2015-2992 …	Nhóm 05 lỗ hổng trên phần mềm Apache (Apache Struts, Kylin, Apache Jserv Protocal,...) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, tấn công XSS.	Đã có thông tin xác nhận và bản vá.
2	D-link	CVE 2020 8861 CVE 2020 8862 CVE 2020 6842 CVE 2020 6841	Nhóm 04 lỗ hổng trên thiết bị D link (D-link DAP 2610, D-link DCH-M225 1.05b01,…) 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
3	Chrome	CVE 2020 6407 CVE 2020 6386 CVE 2020 6418 …	Nhóm 05 lỗ hổng trên trình duyệt web Chrome (Google Chrome trước phiên bản 80.3987.116,…) cho phép đối tượng tấn công tấn chèn và thực thi mã từ xa,	Đã có thông tin xác nhận và bản vá
4	Cisco	CVE 2020 3173 CVE 2020 3170 CVE 2020 3168 …	Nhóm 11 lỗ hổng trên thiết bị Cisco (Cisco FXOS Software, Cisco Discovery Protocol,…) cho phép đối tượng tấn công chèn và thực thi mã tùy ý, tấn công từ chối dịch vụ.	Chưa có thông tin xác nhận và bản vá
5	Wordpress	CVE 2019 19134 CVE 2019 17229 CVE 2020 9394 …	Nhóm 10 lỗ hổng trên phần mềm Wordpress (WPJobBoard plugin,…) cho phép đối tượng tấn công tấn công XSS, tấn công CSRF, thực hiện tấn công CSV Injection.	Đã có thông tin xác nhận và bản vá
6	Apple	CVE 2020 3826 CVE 2020 3872 CVE 2020 3837 …	Nhóm 44 lỗ hổng trên sản phẩm Apple (iPadOS 13.3.1, iOS 13.3.1,…) cho phép đối tượng tấn công tấn công chèn và thực thi mã từ xa.	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	atomictrivia.ru
2	iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
3	ydbnsrt.me
4	tttta.sssaaaas.io
5	xdqzpbcgrvkj.ru
6	xjpakmdcfuqe.in
7	amnsreiuojy.ru
8	xjpakmdcfuqe.com
9	xjpakmdcfuqe.biz
10	www.cityofangelsmagazine.com

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.