BẢN TIN NỘI BỘ

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

1. Ban Cơ yếu Chính phủ chịu trách nhiệm bảo vệ bí mật nhà nước trong lĩnh vực cơ yếu

Để nâng cao trách nhiệm và hiệu quả trong công tác bảo vệ bí mật nhà nước, Luật Bảo vệ bí mật nhà nước dành một chương (Chương IV) quy định trách nhiệm bảo vệ bí mật nhà nước của cơ quan, tổ chức. Trong đó, Ban Cơ yếu Chính phủ đảm nhiệm công tác bảo vệ bí mật nhà nước trong lĩnh vực cơ yếu.

Đồng thời, Ban Cơ yếu Chính phủ cũng tham mưu giúp Chính phủ xây dựng và phát triển hệ thống thông tin mật mã quốc gia; quản lý hoạt động nghiên cứu, sản xuất, cung cấp và sử dụng sản phẩm mật mã để bảo vệ thông tin bí mật nhà nước.

Trách nhiệm bảo vệ bí mật nhà nước của cơ quan, tổ chức

Theo Luật Bảo vệ bí mật nhà nước, Chính phủ thống nhất quản lý nhà nước về bảo vệ bí mật nhà nước.

Bộ Công an chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về bảo vệ bí mật nhà nước và có nhiệm vụ, quyền hạn như sau: Xây dựng, đề xuất chủ trương, chính sách, kế hoạch và phương án bảo vệ bí mật nhà nước; Chủ trì xây dựng và trình cơ quan có thẩm quyền ban hành hoặc ban hành theo thẩm quyền văn bản quy phạm pháp luật về bảo vệ bí mật nhà nước; Hướng dẫn thực hiện công tác bảo vệ bí mật nhà nước; Tổ chức bồi dưỡng nghiệp vụ, kiến thức bảo vệ bí mật nhà nước; Phòng, chống vi phạm pháp luật về bảo vệ bí mật nhà nước; Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về bảo vệ bí mật nhà nước; Thực hiện hợp tác quốc tế về bảo vệ bí mật nhà nước theo phân công của Chính phủ; Quy định mẫu dấu chỉ độ mật, văn bản xác định độ mật, hình thức khác chỉ độ mật và mẫu giấy tờ về bảo vệ bí mật nhà nước.

Văn phòng Trung ương Đảng và các Ban đảng, đảng đoàn, ban cán sự đảng và đảng ủy trực thuộc trung ương; cơ quan trung ương của tổ chức chính trị - xã hội, tổ chức xã hội; Hội đồng Dân tộc, Ủy ban của Quốc hội, cơ quan thuộc Ủy ban Thường vụ Quốc hội, Văn phòng Quốc hội; Văn phòng Chủ tịch nước; Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ; Tòa án nhân dân tối cao; Viện kiểm sát nhân dân tối cao; Kiểm toán nhà nước; tỉnh ủy, thành ủy, Đoàn đại biểu Quốc hội, Hội đồng nhân dân, Ủy ban nhân dân tỉnh, thành phố trực thuộc trung ương, trong phạm vi nhiệm vụ, quyền hạn của mình, có trách nhiệm sau đây: Tổ chức thực hiện công tác bảo vệ bí mật nhà nước; Chủ trì xây dựng và trình cơ quan có thẩm quyền ban hành hoặc ban hành theo thẩm quyền văn bản chuyên ngành liên quan đến bảo vệ bí mật nhà nước thuộc phạm vi quản lý phù hợp với quy định của Luật này; Ban hành và tổ chức thực hiện quy chế bảo vệ bí mật nhà nước của cơ quan, tổ chức, địa phương; Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về bảo vệ bí mật nhà nước đối với cơ quan, tổ chức, cá nhân trực thuộc; Phân công người thực hiện nhiệm vụ bảo vệ bí mật nhà nước, thực hiện chế độ báo cáo về công tác bảo vệ bí mật nhà nước theo quy định của Chính phủ. (1)

Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về bảo vệ bí mật nhà nước thuộc phạm vi quản lý và thực hiện trách nhiệm theo quy định (1).

Tại Điều 25 và Điều 26 của Luật Bảo vệ bí mật nhà nước cũng quy định cụ thể về trách nhiệm của người đứng đầu cơ quan, tổ chức trực tiếp quản lý bí mật nhà nước và trách nhiệm của người tiếp cận, người trực tiếp quản lý bí mật nhà nước như sau:

Trách nhiệm của người đứng đầu cơ quan, tổ chức trực tiếp quản lý bí mật nhà nước

Người đứng đầu cơ quan, tổ chức trực tiếp quản lý bí mật nhà nước có trách nhiệm ban hành nội quy bảo vệ bí mật nhà nước trong cơ quan, tổ chức, trừ cơ quan, tổ chức theo quy định (1). Đồng thời, có trách nhiệm chỉ đạo, kiểm tra, đôn đốc việc thực hiện quy định của pháp luật và quy chế, nội quy về bảo vệ bí mật nhà nước trong cơ quan, tổ chức thuộc phạm vi quản lý; Chỉ đạo xử lý và kịp thời thông báo với cơ quan có thẩm quyền khi xảy ra lộ, mất bí mật nhà nước thuộc phạm vi quản lý.

Tổ chức thu hồi tài liệu, vật chứa bí mật nhà nước khi người được phân công quản lý bí mật nhà nước thôi việc, chuyển công tác, nghỉ hưu, từ trần hoặc vì lý do khác mà không được phân công tiếp tục quản lý bí mật nhà nước.

Trách nhiệm của người tiếp cận, người trực tiếp quản lý bí mật nhà nước

Người tiếp cận bí mật nhà nước có trách nhiệm: Tuân thủ quy định của pháp luật, quy chế, nội quy của cơ quan, tổ chức về bảo vệ bí mật nhà nước; Thực hiện các biện pháp bảo vệ bí mật nhà nước; Sử dụng bí mật nhà nước đúng mục đích; Thực hiện yêu cầu và hướng dẫn của cơ quan, tổ chức trực tiếp quản lý bí mật nhà nước.

Đối với người trực tiếp quản lý bí mật nhà nước có trách nhiệm: Thực hiện trách nhiệm của người tiếp cận bí mật nhà nước; Đề xuất người có thẩm quyền quyết định áp dụng các biện pháp để bảo vệ bí mật nhà nước do mình trực tiếp quản lý; Trường hợp phát hiện vi phạm trong hoạt động bảo vệ bí mật nhà nước thì người trực tiếp quản lý bí mật nhà nước phải có biện pháp xử lý và báo cáo người có trách nhiệm giải quyết, thông báo cho cơ quan, tổ chức xác định bí mật nhà nước biết để có biện pháp khắc phục; Trước khi thôi việc, chuyển công tác, nghỉ hưu hoặc vì lý do khác mà không được phân công tiếp tục quản lý bí mật nhà nước thì phải bàn giao bí mật nhà nước cho cơ quan, tổ chức có thẩm quyền quản lý và cam kết bảo vệ bí mật nhà nước đã quản lý.

Link tham khảo: http://antoanthongtin.vn/chinh-sach---chien-luoc/ban-co-yeu-chinh-phu-chiu-trach-nhiem-bao-ve-bi-mat-nha-nuoc-trong-linh-vuc-co-yeu-106006

2. 5 lỗ hổng thực thi mã lệnh từ xa nguy hiểm nhất năm 2020

Thực thi mã từ xa - Remote Code Execution (viết tắt là RCE) là loại lỗ hổng nguy hiểm nhất, cho phép hacker chiếm quyền điều khiển máy chủ ứng dụng, từ đó có thể lấy các dữ liệu quan trọng của doanh nghiệp.

Dưới đây là top 5 lỗ hổng RCE nguy hiểm mới được phát hiện từ đầu năm 2020 do chuyên gia của Công ty cổ phần an ninh mạng Việt Nam (VSEC), đánh giá dựa trên độ phức tạp, sự phổ biến và quy mô tác động của những lỗ hổng này.

- *CVE 2019-2725: Lỗ hổng thực thi mã từ xa trên Oracle weblogic*

Cụ thể, lỗ hổng bảo mật này nằm trong thành phần WLS9-ASYNC trên máy chủ Weblogic của Oracle cho phép kẻ tấn công nhập dữ liệu XML độc hại thông qua đường dẫn được thiết kế đặc biệt mà không cần bất kỳ quyền nào, từ đó có thể xâm nhập và thực thi các mã lệnh tùy ý lên máy chủ Weblogic.

Lỗ hổng này dễ bị kẻ tấn công khai thác, vì bất kỳ ai có quyền truy cập HTTP vào máy chủ WebLogic đều có thể thực hiện một cuộc tấn công. Do đó, lỗi này có điểm CVSS là 9,8/10.

Theo các chuyên gia bảo mật VSEC, khi một tin tặc khai thác được lỗ hổng bảo mật này sẽ có thể xâm nhập vào hệ thống máy chủ, sau đó thực hiện nhiều cuộc tấn công khác như tấn công lừa đảo, gián điệp… và đặc biệt là phát tán các mã độc ransomware (phần mềm độc hại có mục đích tống tiền người dùng).

Hiện nay đã có bản vá cho lỗ hổng này, các chuyên gia VSEC khuyến cáo các quản trị hệ thống nên cập nhật phiên bản mới nhất của Oracle weblogic. Ngoài ra, cần vô hiệu hóa module ASYNC để người dùng có thể chặn tin tặc truy cập vào.

- *CVE 2020-0796: Lỗ hổng thực thi mã lệnh từ xe trên giao thức SMB của Window*

CVE 2020-0796 (RCE) là lỗ hổng thực thi mã từ xa mà không cần xác thực trên Windows 10. Đây được đánh giá là lỗi nghiêm trọng cao nhất trong kiểm thử ứng dụng/phần mềm và có thể tự động lây lan từ một máy tính bị nhiễm sang máy tính khác.

Lỗ hổng này còn gọi là SMBGhost được phát hiện từ đầu tháng 3.2020 nằm trong giao thức SMBv3, và ảnh hưởng đến các phiên bản Windows 10, Core Windows Server, version 1903 và 1909.

SMB (Server Message Block) chạy trên cổng 445, là một giao thức mạng hỗ trợ việc chia sẻ file, duyệt mạng, in và giao tiếp qua mạng. Lỗ hổng bắt nguồn từ cách thức SMBv3 xử lý các truy vấn của tính năng nén dữ liệu phần header (compression header), cho phép kẻ tấn công từ xa có thể thực thi mã độc trên máy chủ hoặc máy khách với đặc quyền trên cả hệ thống.

Hiện nay Microsoft đã ra phiên bản vá lỗ hổng này, chuyên gia VSEC khuyến cáo người dùng và quản trị viên cần cập nhật phiên bản mới và tắt SMBv3 để tránh tin tặc truy cập vào.

- *CVE 2020-1938: Lỗ hổng Ghostcat đọc và chèn tập tin trên Apache Tomcat*

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

Lỗ hổng Ghostcat được đặt tên mã CVE-2020-1938 với điểm 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. Ngoài ra, để lỗ hổng này có thể trở thành Remote Code Execution nếu như trang web cho phép người dùng tải tệp lên.

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.

Chuyên gia 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.

- *CVE-2020-7961: Lỗ hổng chuyển đổi cấu trúc dữ liệu không đáng tin cậy trên Liferay*

CVE-2020-7961 là lỗi chuyển đổi cấu trúc dữ liệu trên nền tảng Liferay - một cổng thông tin mã nguồn mở được sử dụng rộng rãi. Lỗ hổng này cho phép kẻ tấn công lợi dụng các hàm chuyển đổi cấu trúc dữ liệu mà Liferay sử dụng để chèn mã độc, chiếm quyền điều khiển hoàn toàn ứng dụng và thực thi mã lệnh từ xa đến server, thực hiện các hành vi như thay đổi giao diện trang web, đánh cắp dữ liệu...

Lỗ hổng này tồn tại trên các phiên bản Liferay 7.2.1 CE GA2 trở về trước và hiện tại Liferay đã tung ra các bản vá kịp thời ở các phiên bản Liferay Portal 7.1 GA4, 7.0 GA7 và 6.2 GA6.

Chuyên gia VSEC khuyến cáo các doanh nghiệp hiện sử dung nền tảng Liferay cần cập nhật lên các phiên bản mới nhất. Thực hiện cấu hình cho Liferay chỉ được phép sử dụng các hàm chuyển đổi cấu trúc dữ liệu được an toàn.

- *CVE-2019-11469: Lỗ hổng SQL Injection trên ứng dụng ManageEngine Application Manager (MEAM)*

Lỗ hổng SQL Injection tồn tại ở các ứng dụng quản trị hệ thống doanh nghiệp sử dụng ManageEngine Application Manager phiên bản 14072 trở về trước, cho phép kẻ tấn công có thể nhập dữ liệu vào cơ sở dữ liệu của trang web qua các thông số gửi lên server.

Tin tặc sẽ lợi dụng lỗ hổng này để chiếm quyền điều khiển server bằng cách thêm mới một tài khoản quản trị với quyền cao nhất. Vì ManageEngine yêu cầu quyền đăng nhập đến các máy chủ được giám sát, nên hacker dễ dàng có thể chiếm quyền toàn bộ hạ tầng các máy chủ được giám sát bởi ứng dụng MEAM, từ đó có thể trích xuất các dữ liệu quan trọng của hệ thống, cài đặt mã độc trên toàn bộ hệ thống gây thiệt hại nặng nề

Hiện nay, Zoho đã tung ra bản vá cho các phiên bản MEAM. Vì vậy các chuyên gia VSEC khuyến cáo các doanh nghiệp nên cập nhật phần mềm MEAM lên phiên bản mới nhất có thể.

Khuyến nghị: Người quản trị cần kiểm tra và cập nhật các bản vá của các lỗ hổng nêu trên để bảo đảm an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/5-lo-hong-thuc-thi-ma-lenh-tu-xa-nguy-hiem-nhat-nam-2020-1230285.html

3. Phát hiện lỗi bảo mật nghiêm trọng ảnh hưởng hàng tỷ thiết bị chạy Android

Một lỗi bảo mật nghiêm trọng vừa được phát hiện, ảnh hưởng đến hàng tỷ thiết bị sử dụng nền tảng Android, cho phép tin tặc có thể qua mặt và lấy cắp dữ liệu người dùng trên thiết bị.

Các chuyên gia của hãng nghiên cứu bảo mật Promon (Na Uy) vừa phát hiện một lỗ hổng bảo mật nghiêm trọng, có tên gọi Strandhogg 2.0, ảnh hưởng đến các thiết bị đang hoạt động trên nền tảng Android phiên bản 9.0 trở về trước.

Promon ước tính hiện có hơn một tỷ thiết bị chạy Android bị ảnh hưởng bởi lỗi bảo mật nghiêm trọng này.

Lỗ hổng bảo mật Strandhogg 2.0 sẽ cho phép tin tặc tạo ra các ứng dụng độc hại và mạo danh những ứng dụng "sạch", sau đó lừa người dùng đăng nhập vào tài khoản của mình trên những ứng dụng giả mạo này để lấy cắp thông tin đăng nhập, bao gồm thông tin email, tài khoản ngân hàng, mạng xã hội...

Ngoài ra, Strandhogg 2.0 còn cho phép các ứng dụng giả mạo chiếm quyền điều khiển ứng dụng trên Android, từ đó lấy cắp các dữ liệu nhạy cảm của người dùng lưu trên thiết bị như danh bạ, hình ảnh, theo dõi vị trí theo thời gian thực của người dùng…

Tom Lysemose Hansen, nhà sáng lập và Giám đốc công nghệ của Promon, đánh giá lỗi bảo mật Strandhogg 2.0 là rất nguy hiểm vì gần như không thể phát hiện ra được những ứng dụng độc hại khai thác lỗi bảo mật này. Các ứng dụng giả mạo và độc hại có thể hoạt động mà không cần đòi hỏi bất kỳ quyền hạn đặc biệt nào, nên người dùng có thể chủ quan và bị các ứng dụng này qua mặt.

Tuy nhiên, Promon cũng trấn an người dùng chưa cần phải quá lo ngại vì đến nay vẫn chưa có dấu hiệu nào cho thấy tin tặc khai thác lỗ hổng bảo mật Strandhogg 2.0 để thực hiện các hành vi tấn công. Promon không cung cấp thông tin chi tiết về Strandhogg 2.0 vì lo ngại tin tặc có thể lợi dụng để khai thác lỗi bảo mật này, đồng thời gửi thông báo đến cho Google về lỗi bảo mật để sớm phát hành bản vá.

Phát ngôn viên của Google cho biết đã ghi nhận lỗi bảo mật do Promon phát hiện và trấn an người dùng rằng vẫn chưa có bằng chứng nào cho thấy lỗi bảo mật đã bị khai thác.

"Chúng tôi đánh giá cao công việc của các nhà nghiên cứu và đưa ra bản sửa lỗi cho vấn đề mà họ đã phát hiện", phát ngôn viên của Google cho biết.

Hiện tại Google đã tung ra bản vá lỗi nhằm ngăn chặn những ứng dụng giả mạo khai thác lỗi bảo mật Strandhogg 2.0 để xâm nhập vào thiết bị chạy Android của người dùng.

Các chuyên gia bảo mật khuyến cáo người dùng nên nâng cấp thiết bị chạy Android của ngay khi có bản cập nhật mới nhất. Tuy nhiên, một nhược điểm của nền tảng Android đó là các bản cập nhật vá lỗi phát hành sớm hay muộn còn phụ thuộc vào các hãng sản xuất, thay vì có thể nhận các bản cập nhật trực tiếp từ Google (ngoại trừ các thiết bị sử dụng nền tảng Android gốc hoặc do Google phát triển). Do vậy, nhiều khả năng người dùng smartphone chạy Android sẽ phải tiếp tục phải chờ thêm

một khoảng thời gian mới có thể cập nhật bản vá lỗi bảo mật Strandhogg 2.0 trên thiết bị của mình.

Khuyến nghị: Người dùng cần kiểm tra và cập nhật bản vá mới nhất của thiết bị để bảo đảm an toàn thông tin.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/phat-hien-loi-bao-mat-nghiem-trong-anh-huong-hang-ty-thiet-bi-chay-android-644394.html

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	Microsoft	CVE 2020 0901 CVE 2020 1079 CVE 2020 1176	Nhóm 110 lỗ hổng trong các sản phẩm của Microsoft (SharePoint,Dynamics_365, …) cho phép đối tượng tấn công chèn và thực thi mã từ xa, leo thang đặc quyền, tấn công giả mạo XSS, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá.
2	Google	CVE-2020-6476 CVE-2020-6477 CVE-2020-6483 …	Nhóm 35 lỗ hổng trong phần mềm Google Chrome <83.0.4103.61) cho phép đối tượng tấn công thu thập thông tin, tấn công giả mạo, tấn công tràn bộ đệm.	Đã có thông tin xác nhận và bản vá
3	Cisco	CVE-2020-3343 CVE-2020-3344 CVE-2020-3314 …	Nhóm 06 lỗ hổng trong các sản phẩm của Cisco (Cisco AMP, Provisioning, Unified tượng tấn công chèn và thực thi mã từ xa, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
4	IBM	CVE-2020-4286 CVE-2020-4461 CVE-2020-4411 …	Nhóm 06 lỗ hổng trong các sản phẩm của IBM (InfoSphere Information Server, Security Access Manager Appliance,…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã từ xa, tấn công từ chối dịch vụ, tấn công CSRF.	Đã có thông tin xác nhận và bản vá
5	Apache	CVE-2020-1956 CVE-2020-9484 CVE-2020-1955	Nhóm 03 lỗ hổng trong một số thành phần Apache (Kylin, Tomcat, Couchdb) cho phép đối tượng tấn công chèn và thực thi mã từ xa.	Đã có thông tin xác nhận và bản vá
6	Linux	CVE-2020-10711 CVE-2020-12888 CVE-2020-13143	Nhóm 03 lỗ hổng trong hệ điều hành Linux (Linux kernel <5.7) cho phép đối tượng tấn	Đã có thông tin xác nhận và

		…	công truy cập trái phép, tấn công từ chối dịch vụ.	bản vá
7	Netgaer	CVE-2020-11549 CVE-2020-11551 CVE-2020-11550	Nhóm 03 lỗ hổng trong các sản phẩm của Netgear (OrbiTri-Band Business WiFi Add-on Satellite, Outdoor Satellite,BusinessWiFiRouter) cho phép đối tượng tấn công thu thập thông tin, truy cập trái phép, 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	disorderstatus.ru
2	differentia.ru
3	atomictrivia.ru
4	iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
5	ydbnsrt.me
6	xjpakmdcfuqe.com
7	xjpakmdcfuqe.biz
8	0juwrq36.ru
9	hzmksreiuojy.ru
10	xdqzpbcgrvkj.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.