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

1. Cục An toàn thông tin cảnh báo nguy cơ từ phần mềm Zoom

Ngày 14/4/2020, Cục An toàn thông tin, Bộ TT&TT đã phát cảnh báo các Bộ, ngành, địa phương và các tổ chức, cá nhân về nguy cơ mất an toàn thông tin từ phần mềm họp trực tuyến Zoom. Theo đó, các cơ quan, tổ chức hành chính nhà nước không nên sử dụng phần mềm Zoom để phục vụ các buổi họp trực tuyến tại đơn vị mình.

Hiện nay, Zoom đang là phần mềm phổ biến cho việc học trực tuyến, tổ chức hội họp khi làm việc từ xa. Tuy nhiên, phần mềm này tồn tại một số lỗ hổng bảo mật nghiêm trọng như mã hóa dữ liệu đầu cuối yếu, dễ dàng bị dò quét ID cuộc họp, tồn tại lỗ hổng liên quan đến đường dẫn UNC (Universal Naming Convention).

Ông Nguyễn Khắc Lịch, Phó Cục trưởng Cục An toàn thông tin cho biết, ngày 14/4/2020, Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam ghi nhận, có hơn 500.000 tài khoản Zoom đã bị lộ lọt thông tin cá nhân của người sử dụng. Trong đó, bao gồm email, mật khẩu, đường dẫn URL các cuộc họp và mật khẩu kèm theo.

Từ đầu năm 2020, nhiều lỗ hổng bảo mật của Zoom đã được công bố mã lỗ hổng. Trong đó, có lỗ hổng chưa được nhà cung cấp xử lý triệt để, như: CVE-2020-11500, CVE-2020-11469, CVE-2020-11470… với nhiều mức độ nguy hiểm khác nhau.

Thông qua những lỗ hổng trên, tin tặc có thể truy cập bất hợp pháp vào các phòng họp, theo dõi, truyền bá các thông tin xấu, đánh cắp thông tin hoặc cài đặt mã độc trực tiếp trên máy tính người dùng.

Nhằm tăng cường công tác bảo đảm an toàn, an ninh mạng, đặc biệt là bảo vệ thông tin cá nhân, bảo vệ quyền và lợi ích hợp pháp của các cơ quan, tổ chức, doanh nghiệp và người sử dụng, Cục An toàn thông tin đã đưa ra khuyến cáo về phần mềm Zoom. Cụ thể, các cơ quan, tổ chức hành chính nhà nước được khuyến cáo không nên sử dụng phần mềm Zoom để phục vụ các buổi họp trực tuyến tại đơn vị mình.

Đối với các doanh nghiệp, tổ chức, cá nhân khác, Cục An toàn thông tin cho rằng cần cân nhắc cẩn thận khi sử dụng phần mềm họp trực tuyến Zoom cho các hoạt động học trực tuyến, trao đổi trực tuyến hoặc các tổ chức hội họp khác. Các cơ quan, tổ chức, doanh nghiệp cũng được khuyến nghị ưu tiên lựa chọn các sản phẩm phần mềm học trực tuyến, tổ chức hội họp và làm việc từ xa do doanh nghiệp uy tín sản xuất, đặc biệt là các sản phẩm do doanh nghiệp uy tín trong nước cung cấp như Viettel, VNPT, MobiFone, FPT, VNG, CMC,....

Riêng với các doanh nghiệp cung cấp phần mềm học trực tuyến, tổ chức hội họp và làm việc từ xa, Cục An toàn thông tin đề nghị phải trang bị đầy đủ các tính năng bảo mật cho phần mềm, bảo đảm an toàn thông tin cho người sử dụng và phải có đội ngũ kỹ thuật để hỗ trợ kịp thời cho khách hàng.

Đối với người sử dụng các phần mềm học trực tuyến, tổ chức hội họp và làm việc từ xa, Cục An toàn thông tin khuyến nghị cần chú ý tải phần mềm tải phần mềm từ các nguồn chính thống, thường xuyên cập nhật phiên bản mới nhất của phần mềm;

Không chia sẻ thông tin về phòng họp (ID, mật khẩu) để tránh các trường hợp bị kẻ xấu theo dõi, phá hoại.

Bên cạnh đó, người dùng cần thiết lập các cấu hình bảo mật cao trên các phần mềm họp trực tuyến. Cụ thể, người dùng cần đặt mật khẩu phức tạp cho các buổi họp; Kích hoạt chế độ xét duyệt người tham gia trước khi vào phòng họp; Thiết lập các tính năng quản lý việc chia sẻ màn hình trong buổi họp; Hạn chế việc lưu lại nội dung buổi họp trong trường hợp không cần thiết.

Cục An toàn thông tin cũng lưu ý, với những người dùng đã sử dụng phần mềm Zoom, cần thực hiện ngay việc đổi mật khẩu phức tạp, tránh sử dụng chung mật khẩu với các tài khoản khác.

Trường hợp phát hiện nguy cơ, dấu hiệu lộ, lọt thông tin cá nhân của người sử dụng, cần nhanh chóng khắc phục và kịp thời thông báo cho Cục An toàn thông tin, Bộ TT&TT và các cơ quan chức năng có thẩm quyền liên quan để phối hợp xử lý kịp thời các vấn đề phát sinh.

Khuyến nghị: Toàn thể CCVC, NLĐ không sử dụng phần mềm họp trực tuyến Zoom cho các phiên họp của cơ quan, tuân thủ các quy định để tránh bị lừa đảo và đảm bảo an toàn thông tin.

Link tham khảo: http://antoanthongtin.vn/mat-ma-dan-su/cuc-an-toan-thong-tin-canh-bao-nguy-co-tu-phan-mem-zoom-106025

2. Google Chrome 81 dính lỗi bảo mật nghiêm trọng

Trong thông báo chính thức của đội quản lý chương trình kỹ thuật Google, lỗ hổng xuất hiện trong thành tố nhận diện giọng nói của trình duyệt web Chrome và được gọi tên CVE-2020-6457. Sự cố được các nhà nghiên cứu tại phòng thí nghiệm Qihoo 360 Alpha báo cho Google vào ngày 4.4.

Theo Forbes, nếu kẻ xấu dụ thành công nạn nhân vào một website độc hại nào đó, lỗ hổng "Use after free" (loại lỗi bảo mật cho phép kẻ xấu tấn công sau khi người dùng tương tác với phần mềm độc hại) sẽ được kích hoạt, gây tràn bộ nhớ.

Điều này sẽ dẫn tới các hiểm họa trên máy tính khi kẻ tấn công có thể thực thi mã chiếm quyền trên hệ thống. Do tiềm ẩn khả năng để lại hậu quả nghiêm trọng, Google xếp loại đây là vấn đề an ninh cấp bách.

Tới nay chưa có báo cáo liên quan tới hành vi khai thác hay thiệt hại thực tế do CVE-2020-6457 gây ra. Phía Google cũng lập tức có bản cập nhật bảo mật vá lỗi dành cho trình duyệt web Chrome trước khi công khai sự cố và sẽ phát hành trong vài ngày tới, dành cho cả 3 nền tảng Windows, macOS và Linux.

Người dùng có thể thực hiện kiểm tra thủ công phiên bản Chrome đang sử dụng trong phần Help > About Google Chrome. Phiên bản Chrome an toàn sẽ là 81.0.4044.113. Việc kiểm tra này cũng kích hoạt tính năng tự động cập nhật của trình duyệt (nếu vẫn đang ở phiên bản cũ. Sau khi nâng cấp xong, người dùng cần khởi động lại Chrome để giữ thiết bị an toàn tuyệt đối trước lỗ hổng CVE-2020-6457.

Khuyến nghị: Người dùng cần cập nhật phiên bản mới nhất của trình duyệt Chrome để đảm bảo an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/google-chrome-81-dinh-loi-bao-mat-nghiem-trong-1212513.html

3. Công bố chi tiết cách khai thác lỗ hổng trên VMware vCenter Server

Hãng an ninh Guardicore vừa công bố chi tiết cách khai thác lỗ hổng nghiêm trọng trong VMware vCenter Server có thể bị khai thác để chiếm quyền kiểm soát trên máy chủ VMware.

Đầu tháng 4, VMware thông báo cho khách hàng về bản vá một lỗ hổng nghiêm trọng (CVE-2020-3952) ảnh hưởng đến phiên bản vCenter Server 6.7 trên Windows và các máy ảo. Đây là lỗ hổng làm lộ thông tin liên quan đến Directory Service (vmdir), từ đó hacker có thể giành quyền truy cập dữ liệu nhạy cảm, làm bàn đạp để xâm nhập vCenter Server hoặc các dịch vụ khác tùy vào quá trình xác thực của vmdir.

Theo VMware, vCenter Server chỉ bị ảnh hưởng nếu người dùng cập nhật bản vá bằng cách nâng cấp từ các phiên bản cũ. Nếu người dùng tải bản 6.7 về và cài đặt trực tiếp thì không bị ảnh hưởng bởi lỗi này.

Với bản vá vCenter Server 6.7 được nâng cấp từ các phiên bản cũ, các nhà nghiên cứu của Guardicore phân tích xem bản vá đã xử lý hết các lỗ hổng còn tồn tại hay chưa. Về cơ bản, họ đã tiến hành các bước như sau:

- Cố gắng xác thực kết nối LDAP với vmdir
- Thêm người dùng mới với tên người dùng và mật khẩu được yêu cầu trong tên miền 'cn=NEW_USERNAME,cn=Users,dc=vsphere,dc=local'..
- Thêm người dùng mới vào nhóm 'cn=Administrators,cn=Builtin,dc=vsphere,dc=local'.

Từ các bước trên có thể thấy kẻ tấn công có thể tạo ra một tài khoản với quyền quản trị trên vCenter Directory, cho phép chúng có toàn quyền kiểm soát máy chủ VMware.

Các nhà nghiên cứu của Guardicore nhận định rằng các nhà phát triển của VMware dường như biết về các lỗi này nhưng lại không có biện pháp khắc phục trong một thời gian dài.

Chi tiết về cách thức khai thác lỗ hổng có thể tham khảo tại https://www.guardicore.com/2020/04/pwning-vmware-vcenter-cve-2020-3952/

Người dùng được khuyến cáo nên gỡ bỏ tất cả các bản cài từ 6.7 trở về trước và tải về một bộ cài hoàn toàn mới để xử lý lỗ hổng này.

Khuyến nghị: Người quản trị cần kiểm tra và xử lý các lỗ hổng để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/cong-bo-chi-tiet-cach-khai-thac-lo-hong-tren-vmware-vcenter-server.13499/

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	Gitlab	CVE 2020 10980 CVE 2020 10981 CVE 2020 10975 ...	Nhóm 07 lỗ hổng trong Gitlab (EE/CE 8.0.rc1 12.9, 8.17 12.9,…) cho phép đối tượng tấn công thu thập thông tin, tấn công Path traversal, tấn công SSRF.	Đã có thông tin xác nhận và bản vá.
2	Wordpress	CVE 2020 11548 CVE 2020 11514 CVE 2020 9514 …	Nhóm 10 lỗ hổng trong phần mềm Wordpress (Search Meter plugin, Lead Plus X plugin, Rank Math plugin,…) 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
3	Samsung	CVE 2017 18684 CVE 2018 21058 CVE 2017 18652 …	Nhóm 149 lỗ hổng trong các thiết bị di động của Samsung (N7.x, O8.x, Q10.0,…) cho phép đối tượng tấn công truy cập trái phép, thu thập thông tin, tấn công thực thi mã từ xa. 13 lỗ hổng có CVSS: 10.0 (đặc biệt nghiêm trọng).	Đã có thông tin xác nhận và bản vá
4	Linux	CVE 2019 20636 CVE 2020 11669 CVE 2020 11668 …	Nhóm 09 lỗ hổng trong hệ điều hành Linux (phiên bản <5.4.12, <5.2, <5.6.1) cho phép đối tượng tấn công thu thập thông tin, tấn công thực thi mã từ xa. 01 lỗ hổng có điểm CVSS: 10.0 (đặc biệt nghiêm trọng).	Đã có thông tin xác nhận và bản vá
5	Facebook	CVE 2020 1895 CVE 2020 1885	Nhóm 02 lỗ hổng trong Facebook (Instagram for Android <128.0.0.26.128, Oculus Desktop <1.44.0.32849) cho phép đối tượng tấn công chèn và thực thi mã tùy ý.	Đã có thông tin xác nhận và bản vá

6	IBM	CVE 2020 7633 CVE 2019 4603 CVE 2019 4603 …	Nhóm 16 lỗ hổng trong phần mềm IBM (apiconnect cli plugins <= 6.0.1, RQM, ISIQ,…) cho phép đối tượng tấn công thu thập thông tin, chèn và thực thi mã từ xa, tấn công, truy cập trái phép.	Đã có thông tin xác nhận và bản vá
7	Dell	CVE 2020 5348 CVE 2020 5347 CVE 2020 5330	Nhóm 03 lỗ hổng trong thiết bị của Dell (Dell EMC, Dell Latitude 7202) cho phép đối tượng tấn công thu thập thông tin, thực thi mã từ xa.	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	iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
5	ydbnsrt.me
6	xdqzpbcgrvkj.ru
7	track.saygggames.io
8	xjpakmdcfuqe.in
9	xjpakmdcfuqe.ru
10	amnsreiuojy.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.