BẢN TIN NỘI BỘ

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

1. Hai lỗ hổng thực thi mã trong Drupal được vá

Drupal vừa phát hành bản cập nhật cho Drupal 7, 8.5 và 8.6 để xử lý hai lỗ hổng nghiêm trọng có thể bị khai thác để thực thi mã tùy ý.

Một trong hai lỗ hổng cho phép thực thi mã PHP tùy ý từ xa. Vấn đề này liên quan đến stream wrapper phar được tích hợp trong PHP và cách xử lý các phar:// URI không được xác thực.

Theo khuyến cáo của Drupal, một số mã Drupal (core, contrib và custom) có thể đang xử lý dữ liệu đầu vào không được xác thực đầy đủ của người dùng, từ đó tồn tại nguy cơ bị khai thác. Tuy nhiên, để thực hiện điều này đòi hỏi phải có quyền truy cập của quản trị viên hoặc cấu hình khác biệt.

Để xử lý lỗ hổng, các nhà phát triển hệ thống quản lý nội dung (CMS) đã quyết định thêm .phar vào danh sách các tiện ích mở rộng nguy hiểm. Do đó, tất cả các file .phar được tải lên Drupal sẽ tự động chuyển đổi thành .txt để ngăn chặn việc thực thi mã.

Ngoài ra, Drupal đã quyết định vô hiệu wrapper phar: // trên các trang web Drupal 7 chạy phiên bản PHP trước phiên bản 5.3.3. Wrapper này có thể được kích hoạt lại bằng tay trên các phiên bản PHP trước đó, nhưng điều này dẫn đến nguy cơ tồn tại lỗ hổng. Vì vậy, người dùng được khuyến cáo nên cập nhật phiên bản PHP của mình.

Lỗ hổng thứ hai được vá trong các phiên bản mới nhất của Drupal liên quan đến PEAR Archive_Tar, một thư viện của bên thứ ba để xử lý các file .tar trong PHP. Khai thác lỗ hổng này, bao gồm wrapper phar và một file .tar đặc biệt, có thể dẫn đến việc xóa file tùy ý và thực thi mã từ xa.

Các nhà phát triển của Archive_Tar đã vá lỗ hổng (CVE-2018-1000888) và thư viện này đã được cập nhật trong lõi Drupal để ngăn chặn việc khai thác.

Drupal 8.6.6, 8.5.9 và 7.62 đã vá hai lỗ hổng. Các phiên bản Drupal 8 trước 8.5.x đã ngừng được hỗ trợ nên không còn được nhận các bản cập nhật an ninh.

Cả hai lỗ hổng này đều được phân loại là nghiêm trọng. Tuy nhiên, điều đáng chú ý là Drupal đánh giá các lỗ hổng bảo mật dựa trên Hệ thống chấm điểm của NIST chứ không phải CVSS, hay nói cách khác, lỗi nghiêm trọng thực sự nguy hiểm, chỉ xếp thứ 2 sau mức rất nguy hiểm.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng Drupal cần cập nhật phiên bản mới nhất để tránh nguy cơ mất an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/hai-lo-hong-thuc-thi-ma-trong-drupal-duoc-va.11928/

2. Mất tiền trong thẻ ATM, khách hàng nên làm gì?

Mấy ngày nay, một số báo đưa tin về trường hợp khách hàng tại ngân hàng BIDV bị mất tiền trong tài khoản dù không thực hiện giao dịch. Vụ việc đã gây hoang mang cho nhiều khách hàng, đặc biệt là trong thời điểm Tết Nguyên đán đang cận kề.

Qua sự việc xảy ra, có thể thấy kẻ gian dùng hình thức tấn công skimming. Đây là hình thức tấn công lấy cắp thông tin thẻ ATM lưu trữ trên dải băng từ bằng cách lắp đặt thiết bị trên máy ATM, POS

Các khách hàng thì đứng ngồi không yên, một số thì muốn ra ngân hàng rút toàn bộ tiền trong tài khoản, một số muốn đổi mật khẩu thẻ hoặc khóa thẻ...

Nhận định về vấn đề này, các chuyên gia của WhiteHat cho biết, với những vụ việc kẻ gian dùng hình thức tấn công skimming thì không phải do lỗi từ phía khách hàng. Việc sử dụng thẻ từ với công nghệ bảo mật bằng từ tính và thông tin được lưu trữ trên dải băng từ ở mặt sau thẻ từ lâu đã có những điểm yếu an ninh. Các thông tin lưu trữ trên dải băng từ chỉ được mã hoá một lần và khi quẹt thẻ qua máy thanh toán, cây ATM thông tin sẽ được giải mã.

Chỉ những khách hàng giao dịch tại cây ATM đã bị tấn công mới bị lộ thông tin tài khoản. Nếu bị mất tiền trong tài khoản mà không thực hiện giao dịch, khách hàng cần gọi ngay cho ngân hàng để yêu cầu hỗ trợ xử lý.

Các chuyên gia của WhiteHat cũng khuyến cáo thêm, nếu khách hàng đang nghi ngờ không biết mình có phải là nạn nhân hay không và lo sợ mất tiền trong tài khoản, cần bình tĩnh xử lý theo các bước sau:

Nếu ở gần các cây ATM của ngân hàng đang phát hành thẻ, khách hàng hãy mang thẻ ra cây ATM và tiến hành thao tác đổi lại mã PIN.

Nếu khách hàng đang ở xa, không thể đến cây ATM cần gọi điện cho hotline của ngân hàng, thông báo tạm thời khóa thẻ để đảm bảo an toàn.

Bên cạnh đó, khách hàng cũng cần nâng cao ý thức khi sử dụng thẻ ATM:

Luôn có thói quen đổi mã PIN thẻ ATM hoặc đổi thẻ Visa, Master… định kỳ để đảm bảo an toàn.

Khi giao dịch tại cây ATM khách hàng cần lưu ý: kiểm tra xem có bàn phím giả mạo đè lên phím số thật của cây ATM không (bàn phím bị đẩy lên cao hơn), khe nhét thẻ có bị gắn thêm thiết bị lạ hay không (nhét thẻ vào khó khăn hơn)? Nếu có cần báo ngay cho ngân hàng để xử lý.

Về phía ngân hàng, hiện nay các thẻ ATM sử dụng dải băng từ có tính bảo mật không cao. Do đó để đảm bảo an toàn cho khách hàng, các ngân hàng cần có phương án để nâng cấp các thẻ ATM, dùng các phương thức xác thực mạnh hơn chẳng hạn như thẻ chip. Đây là loại thẻ chứa chip điện tử được xem là một máy tính thu nhỏ và hoàn toàn độc lập, không bị ảnh hưởng bởi tấn công skimming.

Bên cạnh đó, ngân hàng cần nâng cao trách nhiệm tìm hiểu nguyên nhân và xử lý nhanh chóng để Khách hàng yên tâm sử dụng dịch vụ.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần đổi mã PIN thẻ ATM, Visa, Master định kỳ. Khi giao dịch tại cây ATM cần kiểm tra xem có bàn phím giả mạo đè lên phím số thật của cây ATM không, khe cắm thẻ có bị gắn thêm thiết bị lạ hay không, nếu có cần báo ngay cho ngân hàng để xử lý.

Link tham khảo: https://whitehat.vn/threads/mat-tien-trong-the-atm-khach-hang-nen-lam-gi.11930/

3. Adobe vá khẩn cấp 02 lỗi nghiêm trọng trong Adobe Acrobat và Reader

Các lỗi bảo mật Adobe vá khẩn cấp giúp tin tặc khai thác máy tính của bạn chỉ bằng cách mở tệp PDF. Adobe đã phát hành bản cập nhật bảo mật out-of-band để vá hai lỗ hổng nghiêm trọng trong Adobe Acrobat và Reader cho cả hệ điều hành Windows và macOS.

Lỗ hổng đầu tiên, được báo cáo bởi Apelt và có tên CVE-2018-16011, là một lỗi use-after-free có thể dẫn đến việc thực thi mã tùy ý. Kẻ tấn công có thể khai thác lỗ hổng bằng cách lừa người dùng nhấp vào tệp PDF tự tạo, cuối cùng sẽ thực thi mã theo lựa chọn của tin tặc với đặc quyền của người dùng đang đăng nhập, cho phép kẻ tấn công chạy bất kỳ phần mềm độc hại nào trên máy tính của nạn nhân mà không cần cho phép.

Lỗ hổng thứ hai Adobe vá khẩn cấp, được phát hiện bởi Hariri và có tên CVE-2018-19725 là một lỗ hổng bảo mật có thể dẫn đến leo thang đặc quyền. Cả hai lỗ hổng bảo mật được đánh giá là nghiêm trọng nhưng ở mức độ ưu tiên là 2. Điều này có nghĩa là công ty không tìm thấy bằng chứng cho thấy các lỗ hổng này đang bị khai thác.

Các phiên bản phần mềm bị ảnh hưởng gồm Acrobat và Reader DC 2015 phiên bản 2015.006.30461 trở về trước, phiên bản 2017 2017.011.30110 trở về trước và Phiên bản Continuous 2019.010.20064 trở về trước trên cả Windows và macOS. Adobe đã xử lý các lỗ hổng bằng phiên bản mới nhất của Acrobat DC 2015 và Acrobat Reader DC 2015 (phiên bản 2015.006.30464), Acrobat 2017 và Acrobat Reader DC 2017 (phiên bản 2017.011.30113) và Acrobat DC Continent và Acrobat Reader DC Continuous (phiên bản 2019.010.20069) cho Windows và macOS.

Vì các lỗ hổng hiện đã được công khai, các tác nhân đe dọa sẽ nắm cơ hội khai thác nhắm mục tiêu vào máy tính người dùng. Vì vậy, chủ sở hữu máy tính Mac và Windows nên cài đặt các bản vá cho hai lỗ hổng này càng sớm càng tốt.

Adobe thường phát hành các bản cập nhật bảo mật cho phần mềm của mình vào ngày thứ ba thứ hai của tháng, giống như Microsoft, vì vậy bạn có thể đợi bản cập nhật Tuesday Patch của tháng này.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần cập nhật phiên bản mới nhất Adobe Acrobat và Reader để đảm bảo an toàn thông tin.

Link tham khảo: https://securitydaily.net/loi-nghiem-trong-trong-adobe-acrobat-va-reader/

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-2019-0565 CVE-2019-0586 CVE-2019-0539 …	Nhóm 48 lỗ hổng trên một số sản phẩm, ứng dụng của Microsoft (Edge, Internet Explorer ASP.NET, Office, Exchange, SharePoint, Skype, Visual Studio, Windows kernel...) cho phép đối tượng tấn công thực hiện nhiều hình thức tấn công khác nhau: tấn công từ chối dịch vụ, thu thập thông tin, XSS, chèn và thực thi mã lệnh, tấn công leo thang.	Đã có thông tin xác nhận và bản vá
2	IBM	CVE-2018-1859 CVE-2018-1932 CVE-2018-1888	Nhóm 07 lỗ hổng trên một số sản phẩm, ứng dụng của IBM (IBM API Connect, IBM i Access for Windows, Jazz Reporting Service, IBM Spectrum Scale) cho phép đối tượng tấn công thực hiện khai thác lỗi XSS, thu thập thông tin, tấn công leo thang, chèn và thực thi mã lệnh thông qua DLL độc hại.	Đã có thông tin xác nhận và bản vá.
3	Apple	CVE-2018-4043 CVE-2017-2411 CVE-2018-4257 ...	Nhóm 53 lỗ hổng trên một số sản phẩm, ứng dụng Apple (Clean My Mac X, iOS, macOS High Sierra, tvOS, iTunes, iCloud, watchOS, Safari, SwiftNIO) cho phép đối tượng tấn công thực hiện: thu thập thông tin, khai thác lỗi tràn bộ đệm và tấn công leo thang.	Đã có thông tin xác nhận và bản vá. Một số lỗ hổng đã có mã khai thác
4	Aterm	CVE-2018-0634 CVE-2018-0640 CVE-2018-0637	Nhóm 17 lỗ hổng trong dòng Camera Aterm HC100RC của NEC cho phép đối tượng tấn	Đã có thông tin xác nhận và bản vá

		....	công chèn và thực thi lệnh của hệ điều hành qua nhiều thành phần khác nhau, khai thác lỗi tràn bộ đệm.	
5	Cisco	CVE-2018-15464 CVE-2018-15453 CVE-2018-0461 …	Nhóm 17 lỗ hổng trên một số sản phẩm, ứng dụng của Cisco cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, thu thập thông tin nhạy cảm, xem thông tin xác thực ở dạng không mã hóa, tấn công XSS, một số lỗi cho phép chèn và thực thi đoạn mã độc hại.	Đã có thông tin xác nhận và bản vá
6	D-link	CVE-2018-20675 CVE-2018-20674	Nhóm 02 lỗ hổng trên một số dòng sản phẩm của D-Link cho phép đối tượng tấn công thực hiện vượt qua cơ chế xác thực để thực thi lệnh độc hại.	Chưa có thông tin xác nhận và bản vá
7	Google - Chrome	CVE-2018-20070 CVE-2018-6167 CVE-2017-15428 …	Nhóm 84 lỗ hổng trên trình duyệt Chrome cho phép đối tượng tấn công thực hiện thu thập thông tin nhạy cảm, vi phạm chính sách cùng nguồn, khai thác lỗi tràn bộ đệm, chèn và thực thi mã lệnh tùy ý.	Đã có thông tin xác nhận và bản vá
8	Imperva	CVE-2018-5412 CVE-2018-5413 CVE-2018-5403	Nhóm 03 lỗ hổng trên một số sản phẩm của Imperva (Imperva SecureSphere, Imperva SecureSphere gateway) cho phép thực hiện tấn công leo thang (thông qua việc thêm khóa xác thực SSH), chèn và thực thi mã lệnh	Chưa có thông tin xác nhận và bản vá. Đã có mã khai thác

2. Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

STT	**Tên miền/IP**
1	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
2	www.cityofangelsmagazine.com
3	dqrzxapnw.info
4	caarmelcollege.org
5	osheoufhusheoghuesdl.com
6	msjbsiq.com
7	6ae79845b2.pw
8	www.corpnox-technologie.fr
9	nlcfoundation.org
10	ahmedfahmy.name

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.