BẢN TIN NỘI BỘ

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

1. Hơn 23 triệu người vẫn dùng mật khẩu 123456

Theo DigitalTrends, báo cáo mới nhất từ Trung tâm an ninh mạng quốc gia tại Anh (NCSC) đã thống kê từ cơ sở dữ liệu công khai của các tài khoản bị lộ mật khẩu.

Qua đó xác nhận rằng với nhiều người, mật khẩu đơn giản vẫn là điều họ hay chọn, với 23,2 triệu người trên toàn cầu sử dụng chuỗi 123456, đây là mật khẩu dễ đoán phổ biến nhất trong danh sách. Mật khẩu dễ đoán phổ biến kế tiếp là 123456789, tiếp theo sau là password, 1111111 và qwerty.

NCSC đã hợp tác với chuyên gia bảo mật Troy Hunt, người lập website Have I Been Pwned để tìm hiểu thêm về các loại mật khẩu mà nhiều người đang dùng để bảo vệ tài khoản.

Tại website này, người dùng có thể tự khám phá cơ sở dữ liệu như tìm xem bao nhiêu lần mật khẩu đơn giản (hoặc của chính bạn) đã xuất hiện trong danh sách các tài khoản bị tiết lộ từ các vi phạm bảo mật. Ví dụ: nhập vào zxcvbnm, (các chữ cái xuất hiện ở hàng dưới cùng của bàn phím) và bạn sẽ thấy mật khẩu đã xuất hiện trong các vi phạm dữ liệu hơn 575.000 lần.

Chuyên gia bảo mật này cũng đề xuất sử dụng bảo mật xác thực hai bước với mật khẩu và khóa nhận qua ứng dụng, giúp người dùng dễ dàng tránh bị hacker dò ra thông tin bí mật.

Danh sách top 10 mật khẩu dễ đoán phổ biến nhất:

123456
123456789
qwerty
password
111111
12345678
abc123
1234567
password1
12345

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng và quản trị viên cần đặt mật khẩu mạnh và tuân thủ các chính sách đổi mật khẩu theo định kỳ để đảm bảo an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/hon-23-trieu-nguoi-van-dung-mat-khau-123456-1074245.html

2. Mạng di động ảo ITelecom bị hack website ngay ngày đầu ra mắt

Sáng 25/4, Công ty Cổ phần Viễn thông Đông Dương Telecom (Indochina Telecom) vừa chính thức ra mắt dịch vụ viễn thông di động đầu số 087 (mạng di động ITelecom).

Bằng việc ký thỏa thuận hợp tác với Tập đoàn VNPT để sử dụng cơ sở hạ tầng của mạng di động VinaPhone, ITelecom đang tiên phong triển khai mô hình mạng di động ảo MVNO (Mobile Virtual Network Operator) tại Việt Nam.

Tuy vậy, theo ghi nhận của Pv. VietNamNet, chiều 25/4, trang web chính thức của nhà mạng này tại địa chỉ ITelecom.vn đã trở thành đích ngắm bởi giới tin tặc. Theo đó, các tin tặc đã thực hiện một vụ tấn công thay đổi giao diện (Deface) vào website của Đông Dương Telecom và chèn vào đó các nội dung khiêu khích.

Tới thời điểm 18h ngày 25/4, website của Đông Dương Telecom đã dừng hoạt động. Khi truy cập vào trang web này, người dùng nhận được thông báo "Hệ thống đang được cập nhật".

Đến 20h tối ngày 25/4, website của ITelecom đã trở lại hoạt động bình thường.

Nhà mạng ITelecom vẫn chưa đưa ra thông tin chính thức về sự cố này.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/mang-di-dong-ao-itelecom-bi-hack-website-ngay-ngay-dau-ra-mat-526583.html

3. Phát hiện lỗ hổng cực kỳ nghiêm trọng chưa được vá trong máy chủ Oracle WebLogic

Các nhà nghiên cứu vừa công bố về lỗ hổng 0-day cực kỳ nghiêm trọng trong ứng dụng máy chủ Oracle WebLogic. Lỗ hổng có thể đã bị hacker khai thác trong thực tế.

Theo các nhà nghiên cứu, chi tiết lỗ hổng CNVD-C-2019-48814 đã được báo cáo tới Oracle, nhưng công ty vẫn chưa phát hành bản vá. Các phiên bản Oracle WebLogic bị ảnh hưởng bao gồm:

WebLogic 10.X

WebLogic 12.1.3

Theo công cụ tìm kiếm ZoomEye, hơn 36.000 máy chủ WebLogic có thể truy cập công khai trên Internet, tuy nhiên số lượng máy chủ tồn tại lỗ hổng chưa xác định được.

Máy chủ Oracle WebLogic được sử dụng nhiều nhất tại Mỹ và Trung Quốc, tiếp theo là các nước Iran, Đức, Ấn Độ…

Vì Oracle phát hành bản cập nhật an ninh theo quý và các bản vá quan trọng chỉ mới được cập nhật trong tháng 4 này, nên có khả năng chưa có bản vá ngay, trừ khi Oracle quyết định tung ra bản cập nhật an ninh bất thường.

Vì vậy, trước khi có bản vá chính thức, các quản trị viên máy chủ được khuyến cáo thực hiện việc thay đổi cài đặt sau để ngăn chặn tấn công:

Xóa wls9_async_response.war, wls-wsat.war và khởi động lại dịch vụ Weblogic hoặc

Ngăn chặn quyền truy cập vào các đường dẫn /_async/* và /wls-wsat/* URL thông qua kiểm soát chính sách truy cập.

Khuyến nghị:

Phòng ATTT khuyến nghị: Các quản trị viên cần thực hiện các cấu hình như trên và cập nhật bản vá mới nhất chính thức để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/phat-hien-lo-hong-cuc-ky-nghiem-trong-chua-duoc-va-trong-may-chu-oracle-weblogic.12189/

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	IBM	CVE-2019-4202 CVE-2019-4203 CVE-2019-4012 CVE-2019-4178 CVE-2018-1925 ...	Nhóm 07 lỗ hổng trên một số sản phẩm, ứng dụng của IBM (API Connect, DB2 Linux/ Windows, Rational Engineering Lifecycle Manage, IBM SDK, WebSphere Application Server...) cho phép đối tượng tấn công thực hiện thu thập thông tin, khai thác các lỗi tràn bộ đệm để chèn và thực thi mã lệnh, tấn công leo thang.	Đã có thông tin xác nhận và bản vá
2	Jenkins	CVE-2019-10303 CVE-2019-10301 CVE-2019-10302 CVE-2019-10306 …..	Nhóm 8 lỗ hổng trên phần mềm Jenkins (phần mềm sử dụng trong phát triển phần mềm) cho phép đối tượng tấn công thu thập thông tin xác thực lưu trữ trong cấu hình của Plugin, một số lỗ hổng cho phép chèn và thực thi mã lệnh.	Đã có thông tin xác nhận và bản vá
3	Apache	CVE-2019-0228 CVE-2019-0232 …..	Nhóm 02 lỗ hổng trong một số sản phẩm của Apache (JMeter, Solr, Qpid Broker-J, Apache Traffic Server) cho phép đối tượng tấn công thực hiện thu thập thông tin, chèn và thực thi mã lệnh trong phạm vi của ứng dụng.	Chưa có thông tin xác nhận và bản vá.
4	Cisco	CVE-2019-1718 CVE-2019-1840 CVE-2019-1837 ……	Nhóm 32 lỗ hổng trên một số sản phẩm của Cisco (các dòng switch Nexus, NX-OS, FXOS Software,) cho phép truy cập và thông tin nhạy cảm lưu trữ trên hệ thống, chèn và thực thi mã lệnh để chiếm quyền kiểm soát thiết bị.	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	localhost.localdomain
2	n.hmiblgoja.ru
3	ajkeahkcueafuiaeuf.ru
4	mokoaehaeihgiaheih.ru
5	43trfdsds.com
6	iuefgauiaiduihgs.com
7	bszotsjovih.com
8	strikotunrev.top
9	mel.cloudcontentsmak.com
10	d3s1.me

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.