ITRC
مرکز تحقیقات مخابرات ایران

دانشگاه شیراز

مرکز تخصصی آپا درزمینه اختلالات امنیتی مرتبط با بد افزارها

cert@shirazu.ac.ir

آسیب پذیری Adobe Flash, Reader, and Acrobat

تنظیم کننده:

صابر نوروزپورلاری

ویرایش: ۱

شماره سند: VP-89/4-9

www.ircert.cc

ITRC
مرکز تحقیقات مخابرات ایران

دانشگاه شیراز

کد آسیب پذیری: VP-89/4-9

نام محصول آسیب پذیر:

۱- Adobe Flash Player 10.0.45.2 and earlier 10.x versions

۲- Adobe Flash Player 9.0.262 and earlier 9.x versions

۳- Adobe Reader 9.3.2 and earlier 9.x versions

۴-Adobe Acrobat 9.3.2 and earlier 9.x versions

نوع سیستم عامل: ویندوز، لینوکس، Apple Mac OS X

کشف توسط:

تاریخ کشف: June 08, 2010

سطح خطر: متوسط

اثرات:

اگر یک کاربر محتویات فلشی ویژه از پیش ساخته شده (specialy crafted) را باز کند ، یک مهاجم کنترلی ممکن است توانایی اداره اختیاری کدها را داشته باشد.

توضیحات:

مدیریت امنیت Adobe ، آسیب پذیری در Adobe Flash را که Flash player ، Reader و Acrobat را تحت تاثیر قرار داده است توضیح می دهد. این مشکل همچنین ممکن است روی دیگر محصولات که به طور مستقل Flash را پشتیبانی می کنند ، از جمله photoshop ، photo shop lightroom ، Freehand mx ، و Firework ها نیز اثر بگذارد.

یک مهاجم می تواند با متقاعد کردن کاربر برای باز کردن محتویات Flash نقش آسیب پذیری خود را ایفا کند. یک فایل flash به طور معمول بر روی صفحه وب قرار می گیرد، اما می تواند در PDF و دیگر document ها نیز قرار بگیرد یا به صورت یک فایل مجزا ایجاد شود.

همانطور که درAPSA10-01 نوشته شده " گزارشاتی وجود دارد که این آسیب پذیری به صورت خودکار علیه Adobe Flash player و Adobe reader و Acrobat، فعال می شود".

راه حل:

بروز رسانی Flash

مرکز امنیت Adobe بروز رسانی را برای Flash Player 10.1.53.64 or 9.0.277.0 توصیه می کند. این بروز رسانی ، Plugin های مرورگر وب و ActiveX control را نیز بروزرسانی می کند ولی پشتیبانی Flash را در Adobe Reader و Acrobat و دیگر محصولات بروز رسانی نمی کند.

بروز رسانی Acrobat و Reader

بیانیه ی بخش امنیت Adobe بروز رسانی را برای Reader و Acrobat نسخه 9.3.3 یا 8.2.3 را توصیه می کند. این بروز رسانی ، پشتیبانی Flash را در adobe reader و Acrobat نیز بروز رسانی خواهد کرد.

برای اینکه کمتر در معرض آسیب های flash باشیم ، تکنیک های زیر را مد نظر قرار دهید:

Flash را در مرورگر وب خود غیر فعال کنید:

برنامه Flash player را پاک کنید یا اجرای آن را برای برخی سایتها محدود کنید. تا حد ممکن ، فقط Flash هایی که در domain های قابل اعتماد هستند را اجرا کنید. برای اطلاعات بیشتر به مقاله " مرورگر وب خود را امن کنید" مراجعه کنید.

Flashرا در Adobe reader و Acrobat از کار بیاندازید:

غیر فعال کردن Flash در adobe reader حملات ناشی از محتویات فلش که در فایل pdf قرار داده شده را کم می کند. غیر فعال کردن پشتیبانی 3D & Multimedia به طور مستقیم بر روی آسیب پذیری اثر نمی گذارد ، ولی راهی برای کاهش خطرات می باشد. برای غیر فعال کردن پشتیبانی Flash و

3D& multimedia و Adobe reader ، فایل های نام برده شده ی زیر را حذف کنید یا آنها را تغییر نام دهید و یا دسترسی به آنها را را از بین ببرید.

Microsoft Windows
"%ProgramFiles%\Adobe\Reader 9.0\Reader\authplay.dll"
"%ProgramFiles%\Adobe\Reader 9.0\Reader\rt3d.dll"

Apple Mac OS X
"/Applications/Adobe Reader 9/Adobe Reader.app/Contents/Frameworks/AuthPlayLib.bundle"
"/Applications/Adobe Reader 9/Adobe Reader.app/Contents/Frameworks/Adobe3D.framework"

GNU/Linux (locations may vary among distributions)
"/opt/Adobe/Reader9/Reader/intellinux/lib/libauthplay.so"
"/opt/Adobe/Reader9/Reader/intellinux/lib/librt3d.so"

مکان فایل ها برای Adobe Acrobat و یا دیگر محصولات Adobe که شامل Flash و 3D&Multimedia هستند متفاوت می باشد . از کار انداختن این plugin ها کیفیت کار را کاهش می دهد و در برابر محتویات فلش موجود در وب سایت ها محافظت نخواهد شد.

وابسته به جدول بروز رسانی برای محصولات بجز flash player ، پشتیبانی 3D& Multimedia و flash را نیز تا زمانی که به آنها واقعا نیاز نیست غیر فعال کنید.

مانع از باز شدن خودکار pdf ها توسط مرورگر اینترنت شوید:

نصب کننده های Adobe reader و Acrobat ، این پیش فرض را برای مرورگر وب در نظر میگیرند تا Pdf ها را به صورت خودکار اجرا کند و نیازی به پذیرفتن توسط کاربر نباشد. این کار می تواند به گونه امن تری انجام شود ، که به روش زیر کاربر سریع تر به این هدف می رسد.

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\AcroExch.Document.7]
"EditFlags"=hex:00,00,00,00
```

نمایش pdf ها را در مرورگر وب غیر فعال کنید:

جلوگیری از اجراشدن pdf ها در مرورگر وب آسیب پذیری را کاهش می دهد. اگر این کار انجام شود ممکن است آسیب پذیری های آینده را هم کاهش دهد.

برای این که مانع باز شدن pdfها به صورت خودکار در مرورگر وب شوید مراحل زیر را انجام دهید:

۱- Adobe Reader را باز کنید.

۲- منوی Edit را باز کنید.

۳- Preference option را انتخاب کنید.

۴- تیک "Display PDF in Browser" را بردارید.

JavaScript را در Adobe reader و Acrobat غیر فعال کنید:

غیر فعال کردن javascript یک سری حفاظت های اضافی در برابر حمله ها فراهم می کند. از منوی preference می توان Acrobat java script را غیر فعال کرد.

(Edit -> Preferences -> JavaScript; uncheck Enable Acrobat JavaScript).

DEP را در ویندوز فعال کنید:

DEP (Data Execution Prevention) را در نسخه پشتیبانی شده ویندوز فعال نگه دارید.

DEP نباید به گونه ای عمل کند که آسیب های ناشی از کرم ها را رفع کند ولی خود آنها را ازبین نبرد ، اما می تواند اثر کدهای آسیب رسان را در بعضی موارد کاهش دهد. مایکروسافت جزئیات اطلاعات تخصصی درباره DEP را در قسمت تحقیقات امنیتی و دفاعی سایت خود با نام

"Understanding DEP as a mitigation technology" منتشر کرده است. استفاده از DEP باید همراه با وصله های کاربردی که در این نوشته آمده است باشد.

Pdf Document را از منابع غیر قابل اعتماد درخواست نکنید:

Pdf های ناآشنا و غیر منتظره را باز نکنید ، مخصوصا وقتی که بر روی وب سایت ها قرار داشته باشد و یا به نامه الکترونیکی پیوست شده باشد. برای الاعات بیشتر می توانید مطلب زیر را بخوانید:

چرا پیوست نامه های الکترونیکی می تواند خطرناک باشد؟

ویژگی هایی که باعث شده پیوست نامه های الکترونیکی راحت و پرطرفدار باشد، همچنین باعث شده که به این نامه ها به یک ابزار معمول برای مهاجمان تبدیل شود.

- نامه الکترونیکی به راحتی می تواند منتشر شود.

انتشار نامه های الکترونیکی بسیار ساده است و به سرعت می توان سیستم های زیادی را آلوده کرد . بیشتر ویروس ها حتی به دخالت کاربر هم نیاز ندارند و خود ویروس ها رایانه های کاربر را مورد بررسی قرار داده و ایمیل آنها را پیدا کرده و فایلهای آلوده را برای آنها ارسال میکنند.

- تقریبا هر نوع فایل ممی توانمد به نامه الکترونیکی پیوست شوند بنابراین مهاجمان آزادی زیادی در انتخاب ویروسی که می خواهند ارسال کنند دارند.
- برنامه هایی که در زمینه ارسال و دریافت نامه های الکترونیکی کارمی کنند ، ویژگی هایی دارند که کار کاربر را راحت تر می کنند ، از جمله آنها دانلود خودکار پیوست نامه هاست که امکان آلوده سدن سیستم را با هر ویروسی فراهم می کنند.

برای محافظت خود در برابر این آلودگی ها چه باید کرد؟

۱- در باز کردن پیوست نامه ها حتی از افرادی که می شناسید هم دقت کنید.

۲- نرم افزارهایتان را بروز نگه دارید.

۳- حتی اگر ضد ویروس شما ویروسی نبودن فایل پیوست را تایید کرد هم ، با احتیاط با آن برخورد کنید، چرا که برخی ویروس های جدید توسط ضد ویروس ها تشخیص داده نمی شوند.

۴- برای باز کردن فایل های پیوست مراحل زیر را انجام دهید:

a. از بروز بودن ضد ویروس خود اطمینان حاصل کنید.

b. فایل را ابتدا در محلی ذخیره کنید.

c. به طور دستی فایل را ویروس یابی کنید.

d. اگر ویروس یاب ویروسی نبودن فایل ها را تایید کرد آن را باز کنید.

e. دانلود خودکار فایل پیوست را در نرم افزار خود غیر فعال کنید.

۵- برخی ویروس ها در صورتی که شما از حساب مدیریت استفاده نکنید امکان آلوده کردن سیستم را ندارند، پس می توان برای چک کردن پست الکترونیک خود از حساب های محدود شده غیر از حساب مدیریت استفاده کرد.

۶- با فعال کردن فیلتر کردن برخی از پیوست های خاص در نرم افزار خود امنیت سیستم را بالا ببرید.

منابع:

- http://www.adobe.com/support/security/bulletins/apsb10-14.html
- http://www.us-cert.gov/cas/techalerts/TA10-159A.html

مرکز آپای دانشگاه شیراز