باسمه تعالی

آسیب‌پذیری عدم پیکربندی صحیح AFP

(Accessible AFP)

مقدمه

پروتکل AFP یا Apple Filing Protocol یک پروتکل اختصاصی شبکه و در واقع بخشی از Apple File Service (AFS) می‌باشد که سرویس به اشتراک‌گذاری فایل و پرینتر را برای سیستم عامل mac فراهم می‌کند. در سیستم عامل mac از دیگر پروتکل‌های مربوط به سرویس فایل مانند smb، nfs، ftp نیز می‌توان استفاده کرد ولی پروتکل afp از بسیاری از ویژگی‌های منحصربه فرد سیستم‌عامل mac پشتیبانی می‌کند که دیگر پروتکل‌ها قادر به پشتیبانی از آن نیستند. همچنین پروتکل afp دارای ویژگی‌های امنیتی است که می‌تواند دسترسی کاربر به فایل‌های مشخصی را محدود کند.

شرح آسیب‌پذیری

اطلاعات ذخیره شده بر روی منابعی که به اشتراک گذاشته شده‌اند، باید در برابر دسترسی‌های غیرمجاز محافظت شوند. همانند دیگر پروتکل‌های به اشتراک‌گذاری فایل، اگر این پروتکل بر روی یک سیستم در حال اجرا و از طریق اینترنت قابل دسترس باشد، در صورت عدم به کارگیری مکانیزم‌های امنیتی، حمله‌کننده از طریق آن می‌تواند به فایل‌های موجود بر روی سیستم قربانی دسترسی داشته باشد.

راه حل رفع آسیب‌پذیری

در صورتی که نیاز به اشتراک‌گذاری فایل از طریق پروتکل afp بر روی بستر اینترنت وجود داشته باشد، باید مکانیزم‌های امنیتی مربوط به آن به طور صحیح تنظیم شده باشد. پروتکل afp مکانیزم‌های امنیتی را از طریق سه روش ارائه می‌دهد:

- احراز هویت کاربر هنگامی که قصد ورود به سرور را دارد.
- وجود یک رمز عبور دلخواه سخت‌افزاری زمانی که کاربر برای اولین بار قصد دسترسی به آن را دارد.
- کنترل سطح دسترسی به پوشه

در سیستم‌عامل اپل برای احراز هویت بین کلاینت و سرور afp از مدل UAM یا User Authentication Modules استفاده می‌شود. هنگامی که کلاینت در ابتدا به سرور متصل می‌شود، لیست روش‌های UAM که سرور از آن‌ها پشتیبانی می‌کند را درخواست می‌کند و پس از آن امن‌ترین روش با قویترین الگوریتم رمزنگاری که در خود کلاینت نیز از آن پشتیبانی می‌شود را انتخاب می‌کند.

حالت‌های احراز هویت برای این پروتکل در جدول زیر آمده است:

ردیف	وضعیت	عبارت رشته‌ای	توضیحات
۱	بدون احراز هویت	No User Authent	احراز اصالت انجام نمی‌شود. در این حالت UAM به هیچ پارامتر ورودی نیاز ندارد.
۲	کلمه عبور آشکار	Cleartext Password	نام کاربری و کلمه‌عبور به صورت آشکار به کارگزار منتقل می‌شود.
۳	مبادله عدد تصادفی	Randnum Exchange	اعداد تصادفی بین کارگزار و کلاینت مبادله می‌شوند و کلمه‌عبور کاربران روی شبکه به صورت فاش ارسال نمی‌شود. استخراج کلید در این حالت به انداز شکستن رمزگذاری DES پیچیدگی دارد.
۴	تبادل دوطرفه عدد تصادفی	2-Way Randnum	در این حالت هم کاربر احراز اصالت می‌شود و هم کارگزار.
۵	تبادل کلید دیفی-هلمن	DHCAST128	استفاده از پروتکل دیفی-هلمن برای تبادل کلید
۶	کربروس	Client Krb v2	استفاده از تیکت‌های کربروس نسخه ۴ و ۵ در احراز هویت کاربر.
۷	اتصال مجدد	Recon1	استفاده از دستور FPLoginExt برای اتصال مجدد.

پروتکل AFP یک لایه اختیاری برای کنترل دسترسی در نظر گرفته است. در این حالت هر منبع (volume) با یک کلمه‌عبور ۸ کاراکتری امن شده و کاربرانی می‌توانند آن را مشاهده کنند که مقدار آن را داشته باشند.

روش امن‌تر در به کارگیری این پروتکل استفاده از کنترل‌دسترسی پوشه‌هاست. در این حالت سه حق جستجو، خواندن و نوشتن برای هر پوشه در نظر گرفته می‌شود. هر پوشه دارای دو ویژگی Owner و Group نیز می‌باشد. Owner شخص سازنده پوشه می‌باشد و تنها او می‌تواند سایر مجوز ها را تغییر دهد.