باسمه‌تعالی

آسیب‌پذیری عدم پیکربندی صحیح Rsync

(Accessible Rsync)

مقدمه

rsync یک ابزار برای جابجایی و همگام‌سازی فایل‌ها و پوشه‌ها بین سیستم و یک حافظه‌ی خارجی از طریق بستر شبکه می‌باشد. این ابزار بیشتر در سیستم‌های عامل مبتنی بر unix استفاده می‌شود.

شرح آسیب‌پذیری

اگر سرویس rsync به‌درستی پیکربندی نشود و از آن بدون هیچ‌گونه مکانیزم احراز هویت و یا دیگر مکانیزم‌های امنیتی استفاده شود، هر کسی می‌تواند با استفاده از این سرویس به سیستم قربانی فایل ارسال کند و یا فایلی از سیستم وی دریافت کند.

همچنین اگر از الگوریتم‌های رمزنگاری برای انتقال داده‌های مبادله شده استفاده نشود، حمله‌کننده می‌تواند با انجام حمله‌ی MITM ، اطلاعات مبادله شده را استخراج نموده و از طریق این سرویس به فایل‌های سیستم هدف دسترسی پیدا کند.

راه حل رفع آسیب‌پذیری

در سرویس rsync قابلیت ایجاد رمز عبور وجود دارد. البته سرویس rsync به طور معمول برای برقراری ارتباط از طریق بستر شبکه از ssh استفاده می‌کند. اگر به هر دلیلی تنظیمات مربوطه انجام نشده باشد و ترافیک انتقالی به صورت فاش باشد، باید با تغییر فایل تنظیمات این قابلیت به سرویس rsync اضافه شود. البته علاوه بر وجود استفاده از مکانیزم‌های رمزنگاری، باید مکانیزم احراز هویت برای این سرویس نیز در نظر گرفته شود. در صورتی که حمله‌کننده بتواند آدرس سروری که سرویس rsync بر روی آن در حال اجرا می‌باشد را به‌دست آورد و در صورتی که مکانیزم احراز هویتی هم وجود نداشته باشد، می‌تواند دسترسی غیر مجاز به سرور داشته باشد.

تنظیمات مربوط به این سرویس در فایلی به نام rsyncd.conf در پوشه etc ذخیره می‌شود. مقادیر نمونه برای این فایل در شکل زیر آورده شده است:

```
lock file = /var/run/rsync.lock
log file = /var/log/rsyncd.log
pid file = /var/run/rsyncd.pid

[documents]
    path = /home/juan/Documents
```

```
    comment = The documents folder of Juan
    uid = juan
    gid = juan
    read only = no
    list = yes
    auth users = rsyncclient
    secrets file = /etc/rsyncd.secrets
    hosts allow = 192.168.1.0/255.255.255.0
```

همانگونه که مشاهده می‌شود، در تنظیمات فوق آدرس فایلی با نام rsyncd.secrets وجود دارد. این فایل حاوی نام کاربری و کلمه‌عبورِ کاربران مجاز برای استفاده از این سرویس است. برای استفاده از این پروتکل بر روی SSH باید از دستورات زیر استفاده شود.

انتقال یک فایل از سیستم محلی بر روی یک سیستم راه دور:

```
rsync -v -e ssh /home/localuser/testfile.txt
remoteuser@X.X.X.X:/home/remoteuser/transfer
```

انتقال یک فایل از سیستم راه دور بر روی سیستم محلی:

```
rsync -v -e ssh remoteuser@X.X.X.X:/home/remoteuser/transfer/testfile.txt
/home/localuser/
```

همگام سازی یک پوشه محلی روی سرور راه دور:

```
rsync -r -a -v -e ssh --delete /home/localuser/testfolder
remoteuser@X.X.X.X:/home/remoteuser/testfolder
```

همگام‌سازی یک پوشه راه دور روی سیستم محلی:

```
rsync -r -a -v -e ssh --delete remoteuser@X.X.X.X:/home/remoteuser/testfolder
/home/localuser/testfolder
```