باسمه تعالی

آسیب‌پذیری عدم احراز هویت در Memcached

فهرست مطالب

۱ مقدمه

Memcached[۱] یک سیستم کش آزاد، متن‌باز و رایگان تحت لایسنس BSD[۲] است که با کاهش لود پایگاه داده سرعت دسترسی به وب‌سایت‌های داینامیک یا برنامه‌ها را افزایش می‌دهد. این برنامه رکوردهای پایگاه داده‌ای که امکان کش شدن دارند را برای استفاده در کوئری های بعدی در حافظه RAM نگه‌داری می‌کند.

Memcached قابل اجرا بر روی سیستم عامل‌های شبه یونیکس (حداقل Linux و OS X) و ویندوزهای مایکروسافت است. Memcached توسط بسیاری از سرویس‌دهنده‌ها از جمله MocoSpace، YouTube، Reddit و غیره استفاده می‌شود.

برنامه Memcached به عنوان واسطی بین برنامه شما و پایگاه داده مقادیر را به صورت کلید-مقدار در حافظه RAM نگهداری می‌کند و شما قبل از ارسال درخواست به پایگاه داده بررسی می‌کنید که آیا مقدار مورد درخواست شما در Memcached وجود دارد یا خیر. در صورت موجود بودن اطلاعات از Memcached دریافت شده و در غیر این صورت مقدار پس از واکشی از پایگاه داده در کش Memcahched برای استفاده بعدی دخیره می‌گردد.

۲ آسیب پذیری عدم احراز هویت در Memcahched

به طور پیش‌فرض Memcached در پورت TCP 11211 در دسترس عموم است. با وجود مزایای متعدد، امکان استفاده از شبکه راه دور جهت اتصال به Memcached و صدور یک دستور ‘stat’ جهت به دست آوردن اطلاعاتی درباره‌ی خود سرویس یا دستورات دیگر جهت بازیابی اطلاعاتی که توسط این سرویس کش شده است می‌تواند وجود داشته باشد. بسته به هدف وجود این سرویس در زیرساخت‌های شما، سیاست‌های مدیریت اطلاعات و استانداردهای برنامه‌نویسی درون سازمان شما، این سرویس می‌تواند اطلاعات بسیار حساسی را کش کند. یک سرویس در دسترس عموم می‌تواند بدون آگاهی شما اطلاعات حساستان را در اختیار عموم قرار دهد.

با وجود پیکربندی پیش‌فرض Memcached ، این سرویس هرگز نباید در دسترس عموم قرار گیرد و دسترسی به آن باید تنها به شبکه سازمان محدود شود.

---

[۱] مخفف لغت Memory cached

[۲] از جمله پراستفاده‌ترین مجوزهای نرم‌افزارهای آزاد است

از Memcached بیشتر در شبکه‌های قابل اعتماد که مشتریان می‌توانند آزادانه به هر سروری متصل شوند استفاده می‌شود. با این حال، گاهی اوقات Memcached در شبکه‌های غیرقابل اعتماد یا جایی که مدیران می‌خواهند بر روی مشتریانی که متصل هستند اعمال کنترل کنند گسترش می‌یابد که برای این منظور، Memcached می‌تواند با پشتیبانی از احراز هویت اختیاری SASL گردآوری شود. اما پی برده شد که Memcached به نادرستی این احراز هویت را به کار گرفته است و یک مهاجم از راه دور می‌تواند از این مسأله جهت دور زدن احراز هویت SASL به طور کامل استفاده کند. این مسأله محصولات Ubuntu 12.10، Ubuntu 13.04، Ubuntu 13.10 را تحت‌تأثیر قرار داده است.

این آسیب‌پذیری CVE-2013-7239 نام گذاری شده است. نمره CVSS v2 پایه 4.8 به آن اختصاص داده شده است. رشته برداری CVSS آن (AV:A/AC:L/Au:N/C:P/I:P/A:N) است.

۳ محصولات تحت‌تأثیر آسیب‌پذیری

تمام نسخه‌های Memcached تحت‌تأثیر آسیب‌پذیری عدم احراز هویت قرار دارند. محصولات Memcached پیش از 1.4.17 به مهاجمان از راه دور اجازه دور زدن احراز هویت به وسیله ارسال یک درخواست نامعتبر با اعتبارنامه‌های SASL و سپس ارسال درخواست‌های دیگر با اعتبارنامه‌های نادرست SASL را می‌دهند.

۴ بررسی وجود آسیب‌پذیری در سرور

شما می‌توانید با استفاده از دستورات زیر IP سرور خود را تست کنید (<ipaddress> را با آدرس IP سرور خود جایگزین کنید) :

```
echo "stats items" | nc <ipaddress> 11211

OR:
$ nmap -p 11211 <ipaddress> --script memcached-info

This is the output if it's open:

Starting Nmap 6.40 ( http://nmap.org ) at 2015-04-01 10:09 EDT
Nmap scan report for xx.xx.xx.xx
Host is up (0.063s latency).
PORT      STATE SERVICE
11211/tcp open  unknown
| memcached-info:
|   Process ID           1726
|   Uptime               43215969 seconds
|   Server time          2015-04-01T14:09:03
|   Architecture         32 bit
|   Used CPU (user)      0.728889
```

```
|   Used CPU (system)    1.032842
|   Current connections  10
|   Total connections    1678
|   Maximum connections  1024
|   TCP Port             11211
|   UDP Port             11211
|_  Authentication       no
Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

۵ اقدامات جهت مقابله با آسیب‌پذیری

جهت کاهش شدت این آسیب‌پذیری اقدامات زیر را انجام دهید:

- اگر سازمان به Memcached نیاز ندارد باید این سرویس غیرفعال و در نهایت از سرور حذف شود.
- اگر Memcached تنها توسط سروری که در آن سرویس اجرا می‌شود مورد نیاز می‌باشد:

فایل پیکربندی را ویرایش کنید: /etc/sysconfig/memcached

و OPTIONS=”” را به OPTIONS=”-1 127.0.0.1” تغییر دهید و با استفاده از دستور زیر سرویس Memcached را راه‌اندازی مجدد کنید:

service memcached restart

از به روز رسانی سرویس‌هایی که در حال استفاده از این سرویس Memcached از طریق آدرس IP "127.0.0.1" یا "localhost" به عنوان آدرس IP سرور، برای اتصال هستند یا سرویسی که احتمال توقف دسترسی به آن است اطمینان حاصل کنید.

- اگر نیاز به دسترسی دیگر سرورهای درون سازمان به Memcached است:
  - در این مورد بهترین گزینه مسدود کردن دسترسی عموم به این سرویس و دادن اجازه دسترسی تنها از آدرس‌های IP خاص با استفاده از یک بسته فیلترینگ (برای مثال iptables) یا یک دیوارآتش سخت‌افزاری است.
  - این سرویس را در معرض محیط DMZ یا بر روی اینترنت قرار ندهید.
  - Memcached را به نسخه 1.4.17 یا بعدتر ارتقاء دهید.