باسمه تعالی

پروتکل Chargen

معرفی پروتکل Chargen

پروتکل CHARGEN (Character Generator Protocol) یکی از پروتکل‌های مورد استفاده در شبکه اینترنت است که برای مدیریت، اشکال‌زدایی و تست از راه دور استفاده می‌شود. سرویس Chargen بدون توجه به ورودی به سادگی داده را ارسال می‌کند. این پروتکل به حملات شنود و Reflection آسیب‌پذیر می‌باشد. نقاط ضعف این پروتکل امکان ساخت و ارسال بسته‌های اطلاعاتی مخرب به یک هدف واحد را فراهم می‌کند.

آسیب‌پذیری‌های متداول Chargen

سرویس Chargen به منظور انجام سنجش و تست در نظر گرفته شده است و می‌تواند از هر دو پروتکل TCP و UDP استفاده نماید. پس از ایجاد یک اتصال TCP ، سرور شروع به ارسال کاراکترهای دلخواه خود به میزبان می‌کند و این فرایند تا زمان بسته شدن اتصال ادامه می‌یابد. در حالتی که Chargen از UDP استفاده می‌کند، سرور پس از دریافت یک بسته UDP از طرف میزبان، یک بسته UDP حاوی یک شماره تصادفی (بین ۰ تا ۵۱۲) به آن ارسال می‌کند. هر گونه اطلاعات دریافت شده توسط سرور دور انداخته می‌شود. این سرویس می‌تواند در حین ارسال داده از یک سرویس به کامپیوتر یا سرویس دیگر شنود شود. این عمل منجر به یک حلقه بی‌نهایت از ترافیک شبکه و حملات DOS می‌شود.

این پروتکل بر روی دستگاه‌های کپی‌برداری چند منظوره و شبیه به آن به طور پیش‌فرض فعال است و مانند حملات DNS Reflection ، chargen نیز در حملات تشدید می‌تواند استفاده شود. زیرا با ارسال یک درخواست کوچک (از یک آدرس IP جعلی) پاسخی بسیار طولانی بازگشت داده می‌شود. با این روش قربانیان با ترافیک عظیمی از UDP روی پورت ۱۹ مواجه می‌شوند.

از دیگر ویژگی‌های امنیتی این سرویس می‌توان به موارد زیر اشاره نمود:

- فاقد محرمانگی
- فاقد یکپارچگی
- در دسترس بودن آن جزئی است (دارای کارآیی پایین یا وقفه در زمان دسترسی به منابع است).
- پیچیدگی دسترسی بسیار پایینی دارد (شرایط دسترسی تخصصی وجود ندارد و مهارت زیادی برای بهره برداری و سوءاستفاده از آن نیاز نیست).

- احراز هویت مناسب ندارد (برای بهره‌برداری از آسیب‌پذیری، نیازی به احراز هویت نیست).
- این پروتکل به دلیل وجود آسیب‌پذیری ذاتی در طراحی آن، کاربرد کمی دارد و باید در صورت عدم نیاز واقعی به آن، در شبکه غیرفعال گردد.

نحوه تشخیص آسیب‌پذیری شبکه (دستگاه / سرور)

دو نمونه خروجی حاصل از اسکن پورت UDP 19 با استفاده از nmap در ادامه آورده شده است:

۱- زمانی که پورت UDP مورد استفاده Chargen باز است:

```
$ sudo nmap -sU -p19 xx.xx.37.38 -oG -
# Nmap 6.40 scan initiated Wed Apr  2 18:24:52 2014 as: nmap -sU -p19 -oG - xx.xx.37.38
Host: xx.xx.37.38 ()    Status: Up
Host: xx.xx.37.38 ()    Ports: 19/open/udp//chargen///
# Nmap done at Wed Apr  2 18:24:52 2014 -- 1 IP address (1 host up) scanned in 0.18 seconds
```

۲- زمانی که پورت UDP مورد استفاده Chargen بسته است:

```
$ sudo nmap -sU -p19 xx.xx.37.35 -oG -
# Nmap 6.40 scan initiated Wed Apr  2 18:25:30 2014 as: nmap -sU -p19 -oG - xx.xx.37.35
# Nmap done at Wed Apr  2 18:25:33 2014 -- 1 IP address (0 hosts up) scanned in 3.11 seconds
```

نحوه امن‌سازی

با توجه به مطالب بیان شده، باید این سرویس به طور کامل غیرفعال گردد یا حداقل با استفاده از فایروال دسترسی به آن محدود شود. همچنین نباید از این سرویس بر روی سرورهای معتبر استفاده کرد. روش کار برای غیر فعال کردن این سرویس در سیستم‌عامل‌های لینوکس و ویندوز در ادامه توضیح داده شده است:

- Linux Server : در اغلب توزیع‌های سیستم عامل لینوکس، Chargen در inetd یا xinetd قرار دارد. به‌طور پیش فرض این سرویس غیرفعال است.

  برای غیر فعال نمودن این سرویس می‌توان عبارت chargen درون فایل /etc/inetd.conf را کامنت کرده و سپس inetd یا xinetd را مجدداً راه‌اندازی نمود. در برخی از توزیع‌ها نیز می‌توان توسط دستور /etc/init.d/chargen stop سرویس را به‌طور موقت غیرفعال نمود و توسط دستور chkconfig chargen off سرویس را از لیست سرویس‌های اجرا شوده در زمان بوت حذف نمود.

- Windows Server : در سرورهای تحت سیستم‌عامل ویندوز، کلیدهای رجیستری زیر باید با مقدار 0 مقداردهی شوند:

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpChargen
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpChargen

سپس درون cmd باید دستورات زیر وارد شوند:

net stop simptcp
net start simptcp