باسمه تعالی

حملات DDoS با سوءاستفاده از سرویس

X Display Manager

(XDMCP)

سیستم پنجره X (X Window System) یک پروتکل نمایش است که توسط دانشگاه MIT در سال ۱۹۸۴ ابداع شده و از همان ابتدا، ایده تحت شبکه بودن در آن تعبیه شده است. به عبارت دیگر، ارتباط X با صفحه نمایش به جای ارتباط مستقیم، ارتباطی مبتنی بر شبکه است. در X، شبکه شفاف بوده و "جایی که برنامه اجرا می‌شود می‌تواند با جایی که دیده می‌شود تفاوت داشته باشد".

X از مدل سرویس‌گیرنده-سرویس‌دهنده (Client-Server) استفاده می‌کند. سرور X برنامه‌ای است که بر روی رایانه‌ای که دارای نمایشگر و کیبورد است نصب می‌شود. سرور X درخواست‌ها را از کلاینت‌ها دریافت کرده، پس از پردازش، آن‌ها را بر روی صفحه نمایش رسم می‌کند. همچنین سرور X اطلاعات را از ماوس و کیبورد و دیگر دستگاه‌های ورودی دریافت کرده، آن‌ها را برای کلاینت‌ها ارسال می‌کند. یک کلاینت درخواست‌هایی مانند «لطفاً پنجره‌ای با مختصات Y و Z را در صفحه نمایش رسم کنید» را برای سرور X ارسال می‌کند. سرور X این درخواست‌ها را گرفته و سپس پنجره را بر روی صفحه نمایش رسم می‌کند. به عنوان مثالی دیگر، سرور اطلاعات را از ماوس دریافت کرده و سپس پیام‌هایی مانند «کاربر در درحال حرکت دادن ماوس در مختصات Y و Z است» را برای کلاینت‌ها ارسال می‌کند.

X Display Manger یک محیط گرافیکی مدیریت ورود به سیستم در سیستم پنجره X برای شروع ارتباط بر روی X Server می‌باشد. پروتکل XDMCP[1] نیز به منظور دسترسی احراز اصالت شده به سرویس مدیریت نمایش[2] برای نمایش از راه دور طراحی شده است.

کلیه تجهیزاتی که سرویس X Display Manager بر روی آن‌ها فعال بوده و از طریق شبکه اینترنت در دسترس هستند، در معرض حمله DDoS قرار دارند.

[1] X Display Manager Control Protocol
[2] display management services

سرویس X Display Manager از پروتکل UDP و شماره پورت ۱۷۷ استفاده می‌کند. این سرویس بر روی بسیاری از تجهیزات در سطح اینترنت قابل دسترس می‌باشد. با استفاده از این سرویس می‌توان به اطلاعاتی در مورد سیستم هدف دست پیدا کرد.

از این سرویس می‌توان در حملات تقویت ترافیک نیز سوء استفاده کرد. بدین منظور، کوئری مناسبی برای پورت UDP/177 ارسال می‌شود. پاسخ دریافتی یکی از دو نوع Willing یا Unwilling خواهد بود که به ترتیب بیانگر ارائه یا عدم ارائه سرویس X Display Manager است. مستقل از نوع پاسخ ارسالی، ضریب تقویت این روش برابر مقدار ۷ می‌باشد.

تحقیقات نشان داده است که در حال حاضر بر روی حدود ۱۴ میلیون آدرس IP یکتا در سطح جهان این سرویس فعال بوده و امکان سوءاستفاده از آن‌ها در حملات DDOS وجود دارد.

روش امن‌سازی

پیشنهاد می‌گردد که در صورت عدم نیاز، دسترسی به سرویس X Display Manager به شبکه داخلی محدود گردد و از طریق شبکه اینترنت تنها افراد مجاز با آدرس‌های از پیش تعیین شده قادر به دسترسی به آن باشند.