آسیب‌پذیری عدم محدودیت ماشین‌های مقصد در UltraVNC Repeater مربوط به VNC

فهرست مطالب

1 مقدمه

VNC مخفف عبارت Virtual Network Computing می‌باشد که محیط گرافیکی دسکتاپ (Desktop) را تحت پروتکل RFB به شما نشان می‌دهد. در حقیقت، VNC نرم‌افزاری است که از طریق آن می‌توانید دسکتاپ یک کامپیوتر دیگر را مشاهده و اختیار آن را از راه دور به عهده بگیرید. VNC به یک یا چند سیستم‌عاملی محدود نمی‌شود و تحت هر سیستم‌عاملی قابل استفاده است. یک نمایش‌دهنده شبکه مجازی (VNC View) می‌تواند به هر شبکه مجازی سروری متصل شود و آن سرور را هدایت نماید. همچنین سرور اجازه متصل شدن چند کاربر را در یک زمان می‌دهد. VNC در ابتدا توسط شرکت AT&T طراحی و ساخته شد و با مجوز استفاده عمومی (General Public License) منتشر شده است.

2 آسیب‌پذیری عدم محدودیت ماشین‌های مقصد در UltraVNC Repeater مربوط به VNC

UltraVNC Repeater در بین VNC Server و VNC Viewer مانند یک پروکسی عمل می‌کند. آسیب‌پذیری در نسخه‌های قبل از UltraVNC Repeater 1300 آدرس‌های IP مقصد یا پورت‌های TCP را محدود نمی‌کند که این امکان را فراهم می‌آورد تا مهاجمان از راه دور با استفاده از Substring بین آدرس IP و پورت برای دستیابی به یک پروکسی باز تلاش کنند.

3 3 محصولات تحت تأثیر آسیب‌پذیری

نسخه‌های قبل از Ultravnc Repeater 1300

4 اقدامات جهت مقابله با آسیب‌پذیری

- از دیواره آتش جهت مسدود کردن تمام اتصالات به پورت TCP 5901,5500 یا پورت 80 مرورگر، به جز از IPهای قابل اعتماد استفاده کنید.

بروزرسانی به نسخه UltraVNC Repeater 1300