راهنمای مشکل امنیتی

موجود بر روی SNMP

راهنمای مشکل امنیتی موجود بر روی SNMP

تاریخ تنظیم : مرداد ۱۳۹۸

گروه شرکت‌های شاتل

فهرست مطالب

SNMP چیست؟

SNMP (Simple network Management Protocol) پروتکل لایه Application است که امکان نظارت و مدیریت دستگاه‌های واقع در شبکه را فراهم می‌کند و درواقع قسمتی از پروتکل TCP/IP است. این پروتکل توانایی مدیریت و پیدا کردن مشکلات و حل آن‌ها را در شبکه برای مدیران شبکه مهیا می‌کند.

پورت‌های پیش‌فرض مربوط به این سرویس ۱۶۱ و ۱۶۲ است.

اطلاعاتی که می‌تواند از طریق SNMP به اشتراک گذاشته شود وابسته به دستگاهی ست که این پروتکل بر روی آن در حال استفاده است اما به‌صورت کلی می‌توان به اطلاعاتی ازجمله جزئیات سخت‌افزار و نرم‌افزار، رابط‌های شبکه، وضعیت پروتکل‌های شبکه، مشخصات تولیدکننده دستگاه ازجمله Model number و قابلیت‌های دستگاه دست‌یافت. هم‌چنین این امکان فراهم است که تنظیمات بسیاری از دستگاه‌های شبکه را از طریق SNMP انجام داد.

مشکلات امنیتی در زمان استفاده از SNMP

تمامی ویژگی‌های ذکرشده باعث می‌شود که مدیریت و نظارت دستگاه‌ها برای مدیران شبکه آسان‌تر شود اما باوجوداین، باز بودن این پورت درصورتی‌که مورد سوءاستفاده هکرها قرار گیرد می‌توان مشکلات امنیتی زیادی ایجاد کند.

برای پیکربندی و یا غیرفعال کردن SNMP در هر دستگاه می‌تواند به مستندات آن محصول مراجعه بفرمایید.

درصورتی‌که پروتکل SNMP به‌صورت محافظت نشده بر روی دستگاه‌های شما باز باشد، این مورد می‌تواند منجر به سوءاستفاده از شبکه شما برای دسترسی به شبکه‌های موجود در اینترنت شود و سیستم‌های شما در این فعالیت‌های غیرقانونی دخیل باشد! هم‌چنین SNMP حفاظت نشده می‌تواند باعث تخریب شبکه و دستیابی به اطلاعات داخلی شبکه شما نیز بشود.

پیشنهادها

- سعی کنید تمامی دستگاه‌های موجود در شبکه خود را بررسی کرده و درصورتی‌که نیاز به باز بودن این پروتکل بر روی این دستگاه‌ها ندارید، دسترسی مربوط به آن را ببندید.
- درصورتی‌که نیاز است حتماً از این پروتکل استفاده کنید، سعی کنید بر روی فایروال‌های شبکه داخلی خود دسترسی به پورت‌های ۱۶۱، ۱۶۲ و دیگر پورت‌هایی که ممکن است توسط SNMP استفاده شود را محدود کنید.

به‌عنوان‌مثال ترافیک ورودی خود را بر روی IP هایی که مربوط به سرویس‌دهنده‌های خودتان است مجاز کرده و باقی را محدود کنید.

- سعی کنید شبکه جداگانه‌ای برای مدیریت دستگاه‌های شبکه خود از طریق SNMP ایجاد کنید.
- در صورت عدم استفاده از فایروال، می‌توانید در دستگاه‌هایی که قابلیت محدود کردن IP های مقصد و منبع رادارند، این محدودیت را اعمال کنید.
- سعی کنید کلیه ترافیک‌هایی که بر روی SNMP ردوبدل می‌شود را مانیتور کنید.
- با توجه به امنیت‌های تعریف‌شده در ورژن هایی نهایی این پروتکل سعی کنید از SNMP V3 استفاده کنید.
- رمز عبور پیش‌فرض مربوط به این پروتکل را تغییر دهید.