# 2016 年 8 月 12 日，星期五

## 漏洞聚焦：Rockwell Automation MicroLogix 1400 SNMP 凭证漏洞

*漏洞发现者：Patrick DeSantis。*

# 描述

Talos 最近发现了 Allen-Bradley Rockwell Automation MicroLogix 1400 可编程逻辑控制器 (PLC) 中的一个漏洞。如果设备运行受影响的固件版本并使用出厂默认配置，则存在此漏洞。导致此漏洞的原因是一个未记录的 SNMP 社区字符串，攻击者可以利用该字符串获得受影响设备的完全控制权限，从而操纵配置设置、使用攻击者控制的代码替换设备上运行的固件，或者中断设备的运行。根据受影响的 PLC 在工业控制流程中所起的作用，此漏洞可能导致重大危害。

除了“public”（读）和“private”（读/写）这些已记录的默认 SNMP 社区字符串，设备中还存在一个未记录的社区字符串：“wheel”（读/写）。攻击者可以利用该字符串进行未经授权的设备更改，例如修改设置或执行恶意固件更新。此外，该社区字符串还可能被用于访问其他 OID，但是这个风险可能仅限于 Talos 测试的特定使用案例。

# 测试的版本

Allen-Bradley Rockwell Automation MicroLogix 1400 可编程逻辑控制器系统版本 7 - 15.004。

# 总结

过去，针对 SNMPv1 和 SNMPv2c 服务的攻击需要利用默认社区字符串在生产使用环境中的漏洞，或者攻击者必须仔细寻找两个设备之间基于 SNMP 的网络通信，才能获得针对设备发动进一步攻击所需的社区字符串值。

虽然操作人员可以更改受影响设备上的默认 SNMP 社区字符串，但是由于该 SNMP 字符串不是供应商记录的字符串，所以无法有效降低该字符串值在 PLC 部署到生产环境之前遭到更改的可能性，因为大多数操作人员很可能不知道该字符串的存在。考虑到上述问题的严重程度，以及相关功能尚未从受影响设备中删除的事实，我们建议用户采取缓解措施来防止攻击者在生产环境中成功利用此漏洞。有关缓解此漏洞的一些建议，请点击此处。

TALOS-2016-0184 可通过 SID 39876 和 39877 进行检测。

有关此漏洞的完整详细信息，请参阅此处的公告。

发布者：Edmund Brumaghin；发布时间 10:38
标签：零日、ICS、IoT、PLC、Rockwell Automation、SCADA、SNMP、漏洞