IPS漏洞161__UDP__snmp+编号00010145；00010141；00010144

IPS防攻击 zhiliao_94802 2017-11-21 发表

组网及说明

漏洞编号也有，而且扫描的是底层的Linux。就想问问这个能否加固。

问题描述

通过对H3C-IPS（10.223.88.111（112/113/114））进行漏洞扫描发现底层系统为**linux 2.6.9 - 2.6.30；然后发现了SNMP的对应漏洞和漏洞编号。请解答能否进行修复？默认团体名的漏洞不是因为在设备上面配置了默认团体名引起的吧？**

高危险	00010145	SNMP使用默认团体名

中危险	00010141	SNMP不能通知management stations	

	信息	00010144	SNMP服务正在运行

解决方法

第一个 高危险漏洞：

(CVE-1999-0516,CVE-1999-0517)SNMP服务存在可读口令
详细描述： 很多操作系统或者网络设备的SNMP代理服务都存在默认口令。如果您没有修改这些默认口令或者口令为弱口令，远程攻击者就可以通过SNMP代理获取系统的很多细节信息。如果攻击者得到了可写口令，它甚至可以修改系统文件或者执行系统命令。

解决方法：
snmp-agent community read xxx
//避免使用public和private等常见团体字
snmp-agent community write xxxx
//避免使用public和private等常见团体字
snmp-agent sys-info version v3 v2c
//系统应配置为SNMP V2c或以上版本
snmp-agent community read XXXX acl 2000
//只允许特定主机通过SNMP访问网络设备

第二个中危漏洞需要看相关的具体信息，最好有对应的CVE漏洞标号

答案来自于 悠哈悠哈