关于S12500、S9500E、SR8800产品默认开启HTTP服务存在安全隐患的解决方法

软件升级 软件升级 丁志强 2012-06-05 发表

关于S12500、S9500E、SR8800产品默认开启HTTP服务存在安全隐患的解决方法

【产品型号】

S12500/S9500E系列交换机/SR8800系列路由器

【涉及版本】

S12500/S9500E系列交换机：R1335及之后的所有版本

SR8800系列路由器：R3343及之后的所有版本

【问题描述】

S12500/S9500E系列交换机在R1335（含）版本之后，SR8800系列路由器在R3343（含）版本之后，新增WEB网管功能，并默认开启HTTP服务。如果设备配置了用户名/密码和service-type（没有配置web服务），当没有进行访问控制的情况下，任何到S12500/S9500E/SR8800可达的PC，都可以使用已配置的用户名/密码登陆web界面进行控制。无论登陆成功或者失败，在配置service-type中都会自动增加web服务。具体情况如下：

1）设备管理方式配置如下：

```
local-user h3c
  password cipher G`M^B
  authorization-attribute level 3
  service-type telnet
```

2）当通过web尝试登陆或登录成功后配置自动变化如下：

```
local-user h3c
  password cipher G`M^B
  authorization-attribute level 3
  service-type telnet
  service-type web
```

上述版本均存在这样的情况，存在安全隐患，如果S12500/S9500E/SR8800有配置的地址，被扫描到后，可能会被暴力破解。

【原因分析】

该问题为平台问题，在早起版本local user web服务器用的是telnet服务(没有server type web命令），为了保持向前兼容，出现了上述现象。

【规避措施 / 解决方案】

1）在没有具体要求使用WEB网管的局点，请关闭http服务，具体命令：undo ip http enable。

2)配置ACL访问控制，只允许特定IP进行访问。

3)后续研发将针对该问题进行修改。解决的具体版本号请关注版本发布公告。