[2012-03-20]H3C SecBladeSSLVPN-CMW340-E7117版本发布

金山 2012-03-20 发表

H3C SecBladeSSLVPN-CMW340-E7117版本发布

一、 使用范围及配套说明：

H3C SecBladeSSLVPN-CMW340-E7117版本正式发布，使用范围为国内市场。

表1：版本配套表

产品系列	H3C SecBlade
型号	SecBlade SSL VPN
内存需求	2G
FLASH需求	64M
BootROM版本号	1.19
CPLD	3.00
目标文件名称	SecBladeSSLVPN-CMW340-E7117.bin
S75E配套主机软件	S7500E-CMW520-R6626
S95配套主机软件	S9500-CMW310-R1651P05
SR66配套主机软件	SR6600-CMW520-R2603
SR88配套主机软件	SR8800-CMW520-R3345P02
SecCenter配套版本	SecCenter Firewall Manager E0027
备注	无

二、 增减特性说明：

表2：特性变更表

版本号	项目	描述
SecBladeSSLVPN-CMW340-E7117	硬件特性更新	新增特性：无 增加单板：无 删除特性：无
	软件特性更新	新增特性：无 删除特性：无 修改特性：无

三、相比前一版本解决的问题说明：

1. 问题ID—RTOD05553

首次发现版本：SECBLADESSLVPN-CMW340-E7114

问题产生的条件：反复点击导航树中的“本地用户”页签。

问题现象：设备异常重启。

2. 问题ID—RTOD05656

首次发现版本：SECBLADESSLVPN-CMW340-E7116

问题产生的条件：使用Avalanche测试仪对SSL VPN进行压力测试。

问题现象：设备内存泄露，一段时间后停止转发。

3. 问题ID—RTOD05624

首次发现版本：SECBLADESSLVPN-CMW340-E7116

问题产生的条件：在获取证书CRL列表后undo web server。

问题现象：设备异常重启。

4. 问题ID—RTOD05620

首次发现版本：SECBLADESSLVPN-CMW340-E7116

问题产生的条件：使用非授权用户访问域管理页面。

问题现象：用户挂在设备上没有释放，导致无法登录业务页面。

5. 问题ID—RTOD05550

首次发现版本：SECBLADESSLVPN-CMW340-E7114

问题产生的条件：无

问题现象：对于被吊销的证书不能检查出非法。

6. 问题ID—RTOD05561

首次发现版本：SECBLADESSLVPN-CMW340-E7114

问题产生的条件：配置了CRL定期更新

问题现象：10多个小时以后用户使用证书+密码认证无法成功。

7. 问题ID—RTOD05560

首次发现版本：SECBLADESSLVPN-CMW340-E7114

问题产生的条件：无

问题现象：从本机Ping 32000字节的包出去会造成内存泄露，导致接口不再收包。

8. 问题ID—RTOD05532

首次发现版本：SECBLADESSLVPN-CMW340-E7114

问题产生的条件：使用avalanche测试仪长时间打流量

问题现象：设备内存耗尽并挂死。

9. 问题ID—RTOD05614

首次发现版本：SECBLADESSLVPN-CMW340-E7115

问题产生的条件：使用avalanche测试仪打入大量HTTP、HTTPS分片报文

问题现象：一段时间后设备异常重启。

10. 问题ID—RTOD05568

首次发现版本：SECBLADESSLVPN-CMW340-E7114

问题产生的条件：域管理员在配置用户有效期时，设置有效期的月份为2、4、6、9或11月。

问题现象：系统提示无效日期。

11. 问题ID—RTOD05570

首次发现版本：SECBLADESSLVPN-CMW340-E7114

问题产生的条件：无

问题现象：TCP代理模块存在内存重复释放的问题，可能导致系统异常重启。

12. 问题ID—RTOD05548

首次发现版本：SECBLADESSLVPN-CMW340-E7114

问题产生的条件：域管理员使用Radius/LDAP远程认证方式登录设备。

问题现象：无法删除和Radius/LADP相同用户名的本地用户。

13. 问题ID—RTOD05567

首次发现版本：SECBLADESSLVPN-CMW340-E7114

问题产生的条件：在10GE接口上配置arp send-gratuitous-arp命令。

问题现象：没有异常提示，同时也不显示配置信息。

四、版本使用限制及注意事项：

1、Vista系统上IP及TCP接入限制：Vista系统登录用户必须具有Administrator权限，否则客户端启动会因权限不够而失败。

2、SecBlade SSL VPN硬件中的USB为预留模块，目前不支持。

五、 版本存在问题与规避措施：

1. 问题ID—RTOD04491

首次发现版本：SECBLADESSLVPN-CMW340-B7101

问题描述：用户使用TCP接入功能拷贝共享文件夹大文件，无法下载，下载一段时间提示出错。

规避措施：尽量避免下载大文件。

2. 问题ID—RTOD04908

首次发现版本：SECBLADESSLVPN-CMW340-B7101

问题描述：多域管理时，某一个域更新CA和Local证书其他域证书也会更新。

规避措施：确保多域使用的证书为同一个。

3. 问题ID—RTOD05395

首次发现版本：SECBLADESSLVPN-CMW340-E7104

问题描述：通过命令行反复导入证书并用Avalanche打流量情况下，SSL VPN堆栈重启。

规避措施：避免反复导入证书。

4. 问题ID—HSD97343

首次发现版本：SECBLADESSLVPN-CMW340-E7114

问题描述：使用avalanche打秒10000新建连接情况下，反复使能、去使能SVPN服务会导致设备挂死。

规避措施：避免在有比较大的流量情况下反复使能及去使能SVPN服务。

5. 问题ID—RTOD05650

首次发现版本：SECBLADESSLVPN-CMW340-E7116

问题描述：配置证书验证，重启设备之后无法正常登录SSLVPN。

规避措施：重启WEB Server。

六、 升级时注意事项：

请务必参照《H3C SECBLADESSLVPN-CMW340-E7117 版本使用指导书.doc》中的版本升级指导进行升级。

如要完整的了解该版本累计解决的问题，请参看配套的《H3C SECBLADESSLVPN-CMW340-E7117 版本说明书.doc》。