

云下一代防火墙任意文件上传漏洞报告

尊敬的天翼云用户：

您好！

安全测试发现，云下一代防火墙部分版本存在任意文件上传漏洞。攻击者可利用该漏洞进行任意文件上传，造成影响的结果并不是执行脚本文件，而是通过把产品 flash 空间占满，导致其他需要使用 flash 空间的功能不能正常使用。

经过分析与确认，受影响的产品范围为 ECFW6000-5.5R9F3（不含 F3）之前的版本。目前该漏洞已在 R9F3 版本及之后的版本中修复，但存量用户仍存在未修复的情况。如现有云下一代防火墙版本为 R9F3 及之后的版本，则不受上述漏洞影响，版本在 R9F3 之前的云下一代防火墙建议升级到最新版本 R9F5。

【影响版本】

版本号 < ECFW6000-5.5R9F3（不含）

【安全版本】

版本号 ≥ ECFW6000-5.5R9F3

【修复方案】

- 1、登录管理界面，在系统-设备管理-管理员里修改管理员的密码，新密码复杂度建议同时包括大小写字母、特殊符号及数字，长度不低于 8，对新密码做好记录留存。
- 2、在系统-配置文件管理-配置文件列表里选择备份恢复，点击开始备份进行配置保存，随后在界面中选中备份的配置文件进行导出，留存当前的配置文件。
- 3、在系统-升级管理-版本升级里，浏览上传.img 镜像文件，将版本升级至 ECFW6000-R9F5 版本。版本获取请在天翼云官网提交云下一代防火墙工单获取。

【其他注意事项】

- a. 新密码复杂度建议同时包括大小写字母、特殊符号及数字，长度不低于 8，对新密码做好记录留存。
- b. 升级过程会对云下一代防火墙进行重启操作，预计中断业务 10 分钟，请提前做好操作时间（建议在晚上 8 点到 11 点之间进行操作）。
- c. 云下一代防火墙镜像为 R6 版本的需先升级到 R7 版本，再升级到 R9F5 版本。R7 及之后的版本可直接升级到 R9F5 版本，升级前一定要备份、导出配置文件。如有操作问题，可提交工单至云下一代防火墙，由专人进行指导操作。
- d. 云下一代防火墙以主备模式部署时，可先升级备机，待备机升级成功并重启完成后再升级主机。

【产品使用安全建议】

- (1) 将对应型号云下一代防火墙产品升级到推荐的最新版本 R9F5。
- (2) 账号密码：部分用户使用旧版本，登录账密使用的是默认账密，建议用户修改默认账户及密码，使用强账号密码，新密码注意记录留存。
- (3) 登录权限：部分用户使用旧版本或进行远程运维，强制开启云墙 ssh 登录权限，存在远程登录风险。

关闭操作指导：

- 1、登录 Web 界面，进入【网络】 - 【接口】 - 【eth0/0】 - 【编辑】



2、关闭 SSH、Telnet、HTTP 等不安全协议。

Ethernet 接口

接口名称 ethernet0/0

描述 (0 - 63) 字符

绑定安全域 二层安全域 三层安全域 TAP 无绑定

安全域* trust

HA同步

IP配置

类型 静态IP 自动获取 PPPoE

DHCP 服务器提供的网关信息设置为默认网关路由

高级选项 DDNS

管理方式 Telnet SSH Ping HTTP

HTTPS SNMP

WebAuth

认证服务 启用 关闭 使用全局默认

(4) 登录账号：建议使用三权分立及最小权限运维原则进行防火墙运维，禁止 Any 用户登录运维，保障设备管理账号安全。

如需帮助请通过在线工单或 400 热线联系我们，我们将第一时间提供响应和支持。

天翼云服务团队
2022 年 6 月 21 日