

知 H3C ICG系列路由器是否涉及认证绕过和命令注入漏洞

软件相关 刘嘉福 2022-11-16 发表

问题描述

设备开启远程管理功能的情况下，攻击者可发送特殊的请求绕过设备安全认证流程，最终可获取设备管理权限。

解决方法

涉及的产品：H3C ICG800g/ICG800/ICG810/ICG1000/ICG1800

上面的产品涉及，可以通过关闭远程管理功能规避。且属于Miniware，智能终端产品，非Comware的通信网关路由器。

Comware产品统一不涉及，比如ICG3000，6000等产品。

dis version可以查看平台：

```
<H3C>dis version H3C Comware Software, Version 7.1.064, Release 0821P11
```

Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.

