

组网及说明

无

问题描述

- 1、现场有一台SecPath F1060(V7)设备，用别的厂商的设备检测出设备上有漏洞
- 2、现场的漏洞是(CNVD-2020-10223)，显示攻击者可利用该漏洞登录设备获取敏感信息

过程分析

- 1、这个漏洞解释说明如下：

因为我们设备缺省未对用户密码有强度要求（缺省不开启password-control），所以很多用户在开局配置了弱密码后为了方便使用持续使用admin/admin，admin/123456之类的弱密码，并且IP地址暴露在公网上未对源进行限时的时候，攻击者可以通过暴力破解的方式猜解口令。

解决方法

针对这个问题，有如下处理方式

- 1、不使用弱密码
- 2、如果IP地址公网可达，建议限制登录源
- 3、启用password-control