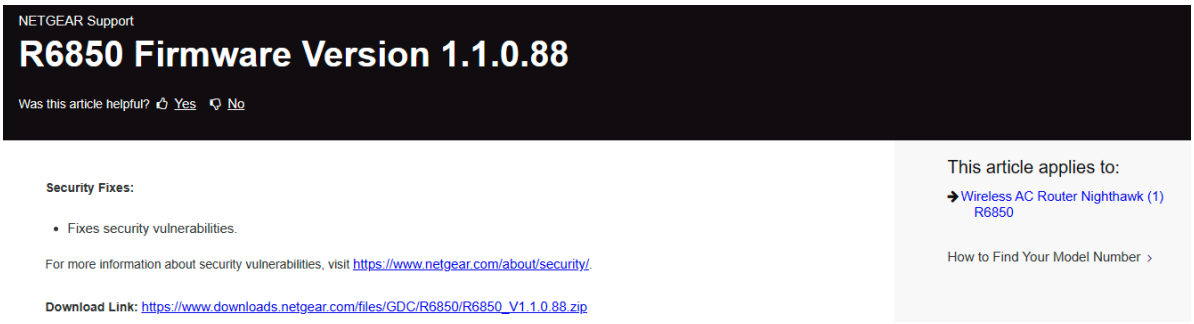
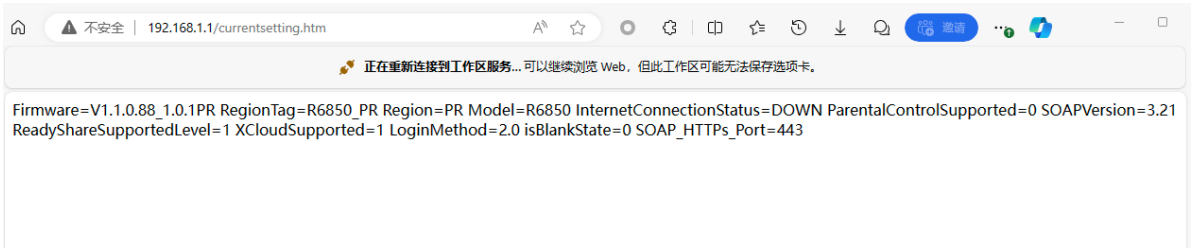
Info Leak in Netgear-R6850 (currentsetting.htm)



Overview

```
* Type: Information leak
* Supplier: Netgear (https://www.netgear.com/)
* Victim URL: http://192.168.1.1/currentsetting.htm
* Product: R6850 – AC2000 Smart WiFi Router
* Affect version: (lastest) 1.1.0.88
* Firmware
download:https://www.downloads.netgear.com/files/GDC/R6850/R6850_V1.1.0.88.zip
```



Description

An infomation leaking vulnerability is at the web management interface of the affected routers. Without any permition, attacker can get sensitive information from the victim URL.

The victime url is a hidden interface and isn't been protected by authentication.

Business Impact

The leaked information is sensitive and could result in serious damage. Thus the vulnerability is very dangerous which could also result in reputational damage for the business through the impact on customers' trust.

Steps to Reproduce

Visit the victime URL from the web, sensitive information is explosed as below:
'''Firmware=V1..0.88 1.0.1PR Regionag=R6850 PR Region=PR Model=R6850 intemetconnectionstatus=DOWN Parentalcontrolsupported=0 SOAPversion=3.21 ReadyshareSupportedLevel=1 XCloudsupported=1 LoginMethod=2.0 isBlankstate=0 SOAP HTTPS Port=443'''