Info Leak in Netgear-R6850 (debuginfo.htm)

NETGEAR Support

R6850 Firmware Version 1.1.0.88

Was this article helpful? 👍 Yes 👎 No

Security Fixes:

- Fixes security vulnerabilities.

For more information about security vulnerabilities, visit https://www.netgear.com/about/security/.

Download Link: https://www.downloads.netgear.com/files/GDC/R6850/R6850_V1.1.0.88.zip

This article applies to:

➜ Wireless AC Router Nighthawk (1) R6850

How to Find Your Model Number ›

Overview

```
* Type: Information leak
* Supplier: Netgear (https://www.netgear.com/)
* Victim URL: http://192.168.1.1/debuginfo.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
```


⌂ ⚠ 不安全 | 192.168.1.1/debuginfo.htm

WAN connection type: Static IP
Product model name: R6850

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: ''' WAN connection type: Static IP Product model name: R6850'''