

[main](#) IoT-CVE / Tenda / AX1806 / 10 /

c0rn-0x2d1 Update README_zh.md ...

on Feb 9 [History](#)

..



image

10 months ago



README.md

10 months ago



README_zh.md

10 months ago



README.md

Affect device: Tenda Router AX1806 v1.0.0.1(<https://www.tenda.com.cn/download/detail-3306.html>)

Vulnerability Type: Heap overflow

Impact: Denial of Service(DoS)

Vulnerability description

This vulnerability lies in the `/goform/saveParentControlInfo` page which influences the latest version of Tenda Router AX1806 v1.0.0.1:

<https://www.tenda.com.cn/download/detail-3306.html>

There is a heap overflow vulnerability in the `saveParentControlInfo` function.

The `v2` variable is obtained directly from the http request parameter `deviceId`.

Then this function calls the `strcpy` function to copy the `v2` to `v5 + 2`.

However, `v5` is a heap address pointer. So it causes heap overflow.

