librick / CVE-2022-41435.md

Last active 14 days ago

☆ Star

<> Code Revisions 2 ☆ Stars 2

CVE-2022-41435

CVE-2022-41435.md

CVE ID: CVE-2022-41435
Name of Affected Product(s): OpenWRT LuCI
Affected Version(s): git-22.140.66206-02913be
Problem Type:

- **Vulnerability Type**:
  Stored XSS via injection of markdown in SSH public key comments
- **Root Cause**:
  The `luci-mod-system` module parses SSH public key information from the file `/etc/dropbear/authorized_keys` within OpenWRT's filesystem but fails to properly sanitize SSH public key comments before the comments are displayed to users

Description:
OpenWRT's default SSH server is dropbear.
dropbear (by default) stores SSH public keys at `/etc/dropbear/authorized_keys`.

When the LuCI SSH page is accessed
(for example, via `System > Administration > SSH-Keys`)
any markdown stored as a comment in any persisted SSH public key
is injected into the page and executed.

This is NOT a vulnerability in dropbear or OpenWRT.
This is a vulnerability in the LuCI `luci-mod-system` module.
See: https://git.openwrt.org/?p=project/luci.git;a=tree;f=modules/luci-mod-system

Additional Information:

The issue was first communicated to the OpenWRT team via the email address provided for responsible disclosure (contact@openwrt.org) on September 20th, 2022.
I communicated with OpenWRT maintainer Jo-Philipp Wich.
The issue was patched by Jo on September 21st, 2022.
See:
https://github.com/openwrt/luci/commit/944b55738e7f9685865d5298248b7fbd7380749e

I contacted MITRE on September 21st, 2022 (after Jo's commit).
I was assigned CVE-2022-41435 on October 14th, 2022.

The following is from my initial CVE request:

> [Suggested description] OpenWRT LuCI git-22.140.66206-02913be was discovered to contain a stored cross-site scripting (XSS) vulnerability in the component /system/sshkeys.js. This vulnerability allows attackers to execute arbitrary web scripts or HTML via crafted public key comments.
>
> [Additional Information] Thanks to Jo on the OpenWRT team for fixing this. I contacted him via the contact@openwrt.org email address and he pushed out a fix promptly (https://github.com/openwrt/luci/commit/944b55738e7f9685865d5298248b7fbd7380749e).
>
> [Vulnerability Type] Cross Site Scripting (XSS) [Vendor of Product] OpenWRT
>
> [Affected Product Code Base] LuCI - git-22.140.66206-02913be
>
> [Affected Component] luci, luci-mod-system, sshkeys.js
>
> [Attack Type] Context-dependent
>
> [Impact Code execution] true

> [Attack Vectors] To exploit this vulnerability, an attacker adds an SSH public key via LuCI with a specially crafted public key comment that contains executable markup. Alternatively, an attacker with write access to the /etc/dropbear/authorized_keys file on an OpenWRT router can add SSH public keys by modifying that file directly with similarly crafted public key comments. In both cases, the embedded markup will execute when the relevant "SSH-Keys" LuCI page is loaded.
>
> [Reference]
> https://github.com/openwrt/luci/commit/944b55738e7f9685865d5298248b7fbd7380749e
>
> [Has vendor confirmed or acknowledged the vulnerability?] true
>
> [Discoverer] Eric McDonald