



Home > Submit > 792252

# Submit #792252: Totolink A7100RU 7.4cu.2313\_b20191024 Command Injection

**Title** Totolink A7100RU 7.4cu.2313\_b20191024 Command Injection

**Description** "A pre-authentication OS command injection vulnerability exists in the `setLedCfg` functionality exposed via the web management interface (`/cgi-bin/cstecgi.cgi`) of the TOTOLINK A7100RU 7.4cu.2313\_b20191024 router. The CGI handler retrieves user-controlled input from the HTTP parameter `enable`, embeds it directly into a shell command string using `sprintf`, and executes it via `CsteSystem()` without any sanitization or escaping. As a result, a remote attacker with network access to the web interface can inject arbitrary shell commands and execute them with root privileges on the device, without authentication. This allows full compromise of the router and, potentially, further compromise of the attached network."

**Source** [https://github.com/Litengzheng/vuldb\\_new/blob/main/A7100RU/vul\\_183/README.md](https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_183/README.md)

**User** Ltzhuster (UID 95786)

**Submission** 03/29/2026 06:14 AM (15 days ago)

**Moderation** 04/12/2026 09:11 AM (14 days later)

**Status** Accepted

**VulDB entry** 356996 [Totolink A7100RU 7.4cu.2313\_b20191024 CGI /cgi-bin/cstecgi.cgi setLedCfg enable os command injection]

**Points** 20

## Community Content

Submissions are made by [VulDB community users](#). VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

## Documentation

- [Submission Policy](#)
- [Data Processing](#)
- [CVE Handling](#)