




Home > Submit > 791271

Submit #791271: Totolink A7100RU 7.4cu.2313_b20191024 Command Injection

Title	Totolink A7100RU 7.4cu.2313_b20191024 Command Injection
Description	<p>A pre-authentication OS command injection vulnerability exists in the 'setUPnPcFg' functionality exposed via the web management interface ('/cgi-bin/cstecgi.cgi') of the TOTOLINK A7100RU 7.4cu.2313_b20191024 router.</p> <p>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.</p> <p>This allows full compromise of the router and, potentially, further compromise of the attached network.</p>
Source	https://github.com/Litengzheng/vuldb_new/blob/main/A7100RU/vul_157/README.md
User	 LizHust2 (UID 95662)
Submission	03/27/2026 04:36 PM (13 days ago)
Moderation	04/08/2026 09:20 PM (12 days later)
Status	Accepted
VulDB entry	398377 [Totolink A7100RU 7.4cu.2313_b20191024 CGI /cgi-bin/cstecgi.cgi setUPnPcFg 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](#)