405 rue Lavoisier
38330 Montbonnot-Saint-Martin
France
Tél. +33 (0) 476 042 000
cyber@etictelecom.com
www.etictelecom.com

ETIC Telecom Security Advisory Report

V2501 Remote Code Execution Vulnerabilities

Publication date: 03/20/2026
Last modified: 03/20/2026

Description

The web administration interface has several Remote Code Execution (RCE) vulnerabilities. An attacker can inject untrusted inputs passed as arguments to the process. If a malicious user manages to inject arbitrary code or commands through these parameters, it can lead to remote code execution, compromising the integrity and security of the system.
Some filters added to prevent the injection of malformed input are bypassable and can cause malicious actions such as a denial of service on the use of the web interface.

Affected products/versions

RAS/IPL/SIG routers with firmware versions prior to 4.13.0.

Severity

CVSS v3.1 Score: **6.2 Medium**
CVSS v3.1 Vector: CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N

Mitigation

For all firmware versions 4.13.0 and above, this issue is fixed.

For versions prior to 4.13.0, to reduce the attack surface, ETIC Telecom advise the user to verify in the router configuration that:

- The administration web page is accessible only through the LAN side over HTTPS.
- The administration web page is protected with authentication.

ETIC Telecom notes

To perform this attack, the attacker must be logged into the administration web page.
Usually, the router services are only reachable on the factory LAN side or through a VPN connection. Thus, the risk of an attack is limited.