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

## V2405 Cross Site Request Forgery

CVE Entry: CVE-2024-26153
Publication date: 12/03/2024
Last modified: 12/03/2024

### Description

The Web administration interface is vulnerable to Cross-Site Request Forgery (CSRF). An external attacker with no access to the device can force the end user into submitting a "setconf" method request, not requiring any CSRF token, which can lead into denial of service on the device.

### Affected products/versions

RAS/IPL/SIG routers with firmware versions prior to 4.9.19.

### Severity

CVSS v3.1 Score: **7.4 High**
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:H

### Mitigations

For all firmware versions 4.9.19 and above, this issue is fixed.

### ETIC Telecom notes

Web sessions are short, lasting only 5 minutes, which reduces the risk of attack. Remember to log out if you no longer use the router.

### Acknowledgments

This vulnerability was independently discovered by two auditors, including Haviv Vaizman, Hay Mizrachi, Alik Koldobsky, Ofir Manzur, and Nikolay Sokolik of OTORIO and Zhouyuan Yang of Fortinet's FortiGuard Labs.