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

V2402 Reflected Cross Site Scripting get_view

CVE Entry: CVE-2024-26157
Publication date: 12/03/2024
Last modified: 12/03/2024

Description

The Web administration interface is vulnerable to Reflected Cross Site Scripting (XSS) attacks in get_view method under view parameter. The ETIC RAS web server uses dynamic pages that get their input from the client side and reflect the input in their response to the client.

Affected products/versions

RAS/IPL/SIG routers with firmware versions prior to 4.5.0.

Severity

CVSS v3.1 Score: **6.1 Medium**
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Mitigations

This issue has been fixed in version 4.5.0. Update to firmware version 4.5.0 and above.

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

ETIC Telecom thanks Haviv Vaizman, Hay Mizrachi, Alik Koldobsky, Ofir Manzur, and Nikolay Sokolik of OTORIO for finding this vulnerability and notifying us.