ETIC Telecom Security Advisory Report

V2403 Persistent Cross Site Scripting site_name

CVE Entry: CVE-2024-26154
Publication date: 12/03/2024
Last modified: 12/03/2024

Description

The Web administration interface is vulnerable to Reflected Cross Site Scripting in the appliance site name. The ETIC RAS web server saves the site name and then presents it to its administrators in few different pages.

Affected products/versions

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

Severity

CVSS v3.1 Score: **4.8 Medium**
CVSS v3.1 Vector: AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N

Mitigations

For all firmware versions 4.5.0 and above, this issue is fixed.

For versions prior to 4.5.0, 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.

Acknowledgments

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

Latest updates are available here: www.etictelecom.com/en/softwares-download