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

V2002 Stored XSS vulnerability

Publication date: <06/01/2022>
Last modified: <06/01/2022>

Description

The web application is vulnerable against stored XSS (Cross-Site Scripting) attacks. Indeed, the device name parameter is not properly sanitized or cleaned by the application, which allows injecting arbitrary JavaScript code to conduct XSS attacks. Since the "HttpOnly" flag is not set in session cookies, an attacker may inject malicious JavaScript code into the vulnerable parameters to steal user sessions to perform session hijacking attacks. In another attack vector, an attacker may redirect ETIC's users to a malicious page to perform phishing attacks.

Affected products/versions

RAS/IPL/SIG routers with firmware versions prior to 4.7.0.

Severity

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

Mitigations

This issue has been fixed in version 4.7.0.

For versions prior to 4.7.0, to reduce the attack surface, we advise 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 stored XSS 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 Digital.Security for finding this vulnerability and notifying us.

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