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

## V2202 Malicious File Upload

CVE Entry: CVE-2022-40981
Publication date: 11/10/2022
Last modified: 11/16/2022

### Description

Vulnerability to malicious file upload. An attacker could take advantage of this to store malicious files on the server, which could override sensitive and useful existing files on the filesystem, fill the hard disk to full capacity, or compromise the affected device or computers with administrator level privileges connected to the affected device.

### Affected products/versions

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

### Severity

CVSS v3.1 Score: **5.9 Medium**
CVSS v3.1 Vector: AV:A/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:L

### Mitigations

For all firmware versions 4.7.0 and above, there is a code signature verification for firmware packages.

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 a malicious file upload, 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.