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

V2201 Directory Traversal

CVE Entry: CVE-2022-41607
Publication date: 11/10/2022
Last modified: 11/16/2022

Description

Application programmable interface (API) is vulnerable to directory traversal through several different methods. This could allow an attacker to read sensitive files from the server, including SSH private keys, passwords, scripts, python objects, database files, and more.

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 directory traversal 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.