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

V2001 Packages with known vulnerabilities

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

Description

The ETIC router exposes several services within the factory network. The embedded system of the router integrates several packages with multiple critical vulnerabilities for these services, which may allow causing Denial of Service attacks (application crash) or even system compromise. These packages imply the SSH administration, the DNS forwarder, the administration web server, and the application web server.

Affected products/versions

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

Severity

CVSS v3.1 Score: **8.2 High**
CVSS v3.1 Vector: AV:A/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:H

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:

- Disable SSH administration server in the configuration (highly recommended).
- Disable DNS forwarder in the configuration.
- Check that the firewall has not been opened to access the web servers directly on the WAN interface.

ETIC Telecom notes

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.