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

V2301 Insecure default initialization of web portal

CVE Entry: CVE-2023-3453
Publication date: 07/27/2023
Last modified: 07/27/2023

Description

The web management portal authentication is disabled by default. This could allow an attacker with adjacent network access to alter the configuration of the device or cause a denial-of-service condition.

Affected products/versions

RAS/IPL/SIG routers with firmware versions prior to 4.9.0.

Severity

CVSS v3.1 Score: **7.1 High**
CVSS v3.1 Vector: AV:A/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L

Mitigations

For firmware versions 4.9.0 or later, enabling the administration protection is mandatory after the first product start.

For firmware versions prior to 4.9.0, we recommend enabling the authentication mechanism on the administration interface.

- This can be done on the page "> Setup > Security > Administration right" by creating an administrator on the "List of administrators" table, enabling the parameter "Password protect the configuration interface,"
- You can also verify that the administration web page is accessible only through the LAN side over HTTPS by setting the parameter "Protocols to use for configuration" to "HTTPs only".

ETIC Telecom notes

Usually, the router web portal is 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.