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

V2404 Clear Text Credentials

CVE Entry: CVE-2024-26155
Publication date: 12/03/2024
Last modified: 12/03/2024

Description

The Web administration interface is exposing clear text credentials. An attacker can access the ETIC RAS web portal and view the HTML code which is configured to be hidden, thus allowing a connection to the ETIC RAS ssh server, which could enable an attacker to perform actions on the device.

Affected products/versions

RAS/IPL/SIG routers with firmware versions prior to 4.5.0.

Severity

CVSS v3.1 Score: **6.8 Medium**
CVSS v3.1 Vector: AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N

Mitigations

For all firmware versions 4.5.0 and above, this issue is fixed.

For versions prior to 4.5.0, to reduce the attack surface, ETIC Telecom advise the user 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 this 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 Haviv Vaizman, Hay Mizrachi, Alik Koldobsky, Ofir Manzur, and Nikolay Sokolik of OTORIO for finding this vulnerability and notifying us.