ETIC Telecom Security Advisory Report

V2203 Privilege Escalation

CVE Entry: CVE-2022-3703
Publication date: 11/10/2022
Last modified: 11/16/2022

Description

Web portal is vulnerable to accepting malicious firmware packages that could provide a backdoor to an attacker and provide privilege escalation to the device.

Affected products/versions

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

Severity

CVSS v3.1 Score: **7.6 High**
CVSS v3.1 Vector: AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H

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:
- That the downloaded firmware comes from a trusted source (https Etic Telecom web site).
- The hash of the firmware files

ETIC Telecom notes

If you have any doubt regarding the firmware file you want to load, contact Etic Telecom technical support.

Acknowledgments

ETIC Telecom thanks Haviv Vaizman, Hay Mizrachi, Alik Koldobsky, Ofir Manzur, and Nikolay Sokolik of OTORIO for finding this vulnerability and notifying us.