Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Vulnerability Note

Asus Armoury Crate AsIO3.sys authorization bypass vulnerability

Vulnerability Note: VN-2025-03

Date of Issue: 17 June 2025

Severity Rating: High

Systems Affected:

- Asus Armoury Crate 5.9.13.0

Description

An authorization bypass vulnerability exists in the AsIO3.sys functionality of Asus Armoury Crate 5.9.13.0. A specially crafted hard link can lead to an authorization bypass. An attacker can create a hard link to trigger this vulnerability.

Armoury Crate is a centralized software application developed by ASUS, designed to manage and customize the settings of ASUS hardware components and peripherals. It provides users with a unified interface to control various features, such as RGB lighting, system performance, fan speeds, and device configurations.

Solution

To mitigate the security problem, it is recommended to apply the latest update by opening the Armoury Crate app and going to "Settings"> "Update Center"> "Check for Updates"> "Update."

More information is available on:
https://rog.asus.com/us/content/armoury-crate/

CVE Information

CVE-2025-3464

References

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwanarbfile-2zKhKZwJ

Postal address

Mauritian Computer Emergency Response Team (CERT-MU)
Ministry of Information Technology, Communication and Innovation
2nd Floor, Wing A,
Shri Atal Bihari Vajpayee Tower,
Cybercity Ebene,