You are here:

ABR-MAC-26-02

This advisory describes a possible local privilege escalationvulnerability in the Admin By Request macOS client.

Notification

Metric	Value
Criticality:	High
Published:	2026-07-01
CVE ID:	CVE-2026-78237
CWE:	TBD
ABR ID:	ABR-MAC-26-02

Rating

Metric	NVD Calculated Rating
CVSS 3.1 Score	7.8

We value your privacy

We use cookies to enhance your browsing experience, serve personalised ads or content, and analyse our traffic. By clicking "Accept All", you consent to our use of cookies.

Customise

Reject All

Accept All

- Exploitation of the vulnerability requires an attacker to have access to the endpoint.
- An attacker must have the ability to programmatically execute the exploit.
- Given the above, an attacker can exploit the vulnerability to gain non-approved elevation.

Description

A vulnerability allowing local privilege escalation has been discovered in the Admin By Request macOS client.

Insufficient input validation in Admin By Request allows a low-privileged user to inject malicious entries into the sudoers file, resulting in persistent root access. The vulnerability requires leveraging the XPC finding in ABR-MAC-26-01.

Mitigation

The affected driver vulnerability has been resolved in **Admin By Request 5.3 for Mac**. Updating to a version >= 5.3 mitigates the vulnerability.

Acknowledgment

Kang Hao Leng, Timothy Lee, Wen Bin Kong from Innoedge Labs

Tan Inn Fung, Sean Seah, Cameron Leong from GovTech Cybersecurity Group (CSG)

Ronald Chia, Manzel Seet from Assurity Trusted Solutions

We value your privacy

We use cookies to enhance your browsing experience, serve personalised ads or content, and analyse our traffic. By clicking "Accept All", you consent to our use of cookies.