Security Advisory

Admin By Request
ZERO TRUST PLATFORM

Product Platform: **Mac**
Product Version: **5.2**
Document Date: **26 August 2026**
Document Version: **1.1**

ABR-MAC-26-02

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

Notification

Metric	Value
Criticality:	**High**
Published:	2026-08-26
CVE ID:	CVE-2026-78237
CWE:	TBD
ABR ID:	ABR-MAC-26-02

Rating

Metric	NVD Calculated Rating
CVSS 3.1 Score	7.8
CVSS 3.1 Vector	AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

This advisory is available online:

Security Advisory: ABR-MAC-26-02

Considerations

Admin By Request's internal assessment scores the risk to be **high** based on the following:

- 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

GovTech Cybersecurity Group (CSG)

Document History

Version	Author	Changes
25 August 2026 **1.0**	Steve Dodson	Initial document release.
26 August 2026 **1.1**	Steve Dodson	Changed the date of publication and updated the *Acknowledgment* section..