Security Advisory

Admin By Request
ZERO TRUST PLATFORM

Product Platform: **Windows**
Product Version: **8.7**
Document Date: **9 March 2026**
Document Version: **1.0**

ABR-WIN-26-01

This advisory describes a possible process spoofing vulnerability in the Admin By Request Windows driver.

Notification

Metric	Value
Criticality	**Medium**
Published:	2026-03-09
CVE ID:	TBD
CWE:	TBD
ABR ID:	ABR-WIN-26-01

Rating

Metric	NVD Calculated Rating
CVSS 3.1 Score	TBD
CVSS 3.1 Vector	TBD

This advisory is available online:

Security Advisory: ABR-WIN-26-01

Considerations

Admin By Request's internal assessment scores the risk to be **medium** 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.

Description

A vulnerability allowing spoofing of a parent process under certain configuration conditions has been discovered in the driver included with the Admin By Request Windows client.

The vulnerability can be leveraged by listening for the elevation driver startup signal and then posing as the driver to elevate non-approved applications or processes.

In order for the vulnerability to be possible, Admin By Request must be configured to use authentication methods other than UAC.

Mitigation

The affected driver vulnerability has been resolved in **Admin By Request 8.7**. The updated driver has also been patched into all prior available versions of Admin By Request for Windows.

There are several options to mitigate the issue depending on preference:

1. Update Windows endpoints to Admin By Request 8.7.
2. Enable the Auto-update feature of Admin By Request.
3. Change Admin By Request authentication settings to "Authenticate".
4. Re-download and re-install a prior version from the Admin By Request portal.
5. Utilize our driver updater utility to update the driver (no re-install required).
6. Manually update the driver file.

Please see "Vulnerability Mitigation Guide" on the next page for more details.

Acknowledgment

Mateusz Paszynski, ProDrive Technologies

Jefferey Hanssen, ProDrive Technologies

Vulnerability Mitigation Guide

Internal Reference: ABR-WIN-26-01

This mitigation guide relates to a possible process spoofing vulnerability in the Admin By Request Windows driver.

Action Required

This vulnerability affects the Admin By Request driver component only. To remediate the issue, please choose one of the following options based on your environment and operational requirements.

Recommended Remediation Options

Option 1: Enable automatic update to version 8.7

In the Admin By Request portal:

1. Go to **Settings > Tenant Settings > Auto-Update > WINDOWS WORKSTATION**.
2. Enable **Auto-update over the internet**.

Once enabled, affected endpoints will be updated to version 8.7, which includes the corrected driver.

Option 2: Upgrade endpoints to version 8.7

Update affected endpoints directly to Admin By Request version 8.7.

Version 8.7 includes the updated driver and fully addresses this vulnerability.

Alternative Mitigation Options

If upgrading to version 8.7 is not currently possible, the following alternatives are available:

Option 3: Change UAC setting to Authenticate

In the Admin By Request portal:

1. Go to **Endpoint Privilege Management > Settings > Windows Settings > Endpoint > UAC**.
2. Change the setting from "Confirm" or "Multi-factor Authentication" to **Authenticate**.

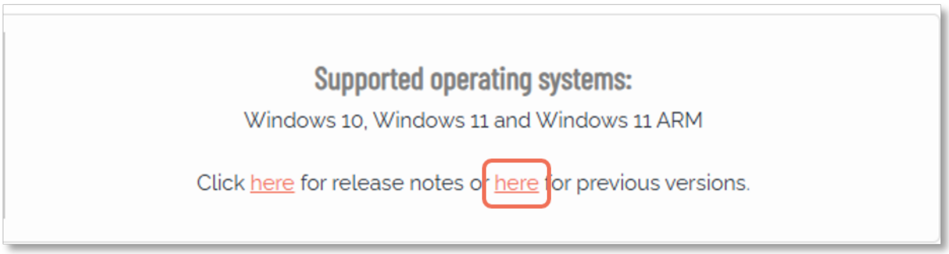
This configuration uses the standard Windows UAC method instead of the Admin By Request driver. As a result, end users will be required to enter credentials when elevating. This can be used as a temporary mitigation.

Option 4: Re-download and reinstall your current version

Re-download the version you are currently using.

In the Admin By Request portal:

1. Go to **Download**.
2. Click the *second* word **here** (as in "here for previous versions"):



Supported operating systems:

Windows 10, Windows 11 and Windows 11 ARM

Click here for release notes or here for previous versions.

3. Download your current version from the list.

For example, if you are using version 8.5, download version 8.5 from the archive, uninstall the existing installation, and then reinstall using the newly downloaded package.

After reinstalling, you can verify that the driver has been updated by using the driver update utility described below.

Option 5: Update the driver only

You may also update the driver independently, without reinstalling Admin By Request. See "Driver Update Program" below.

Option 6: Manually update driver file

Manually push out an updated driver file to affected endpoints. In order to utilize this option, please reach out to our technical support team.

Driver Update Program

The vulnerability has been addressed in version 8.7 through an updated driver. For versions prior to 8.7, the driver can be updated separately by replacing the driver file only. This can be done without reinstalling Admin By Request and without impacting normal product operation.

To support this process, Admin By Request provides a driver update utility that:

- detects the correct platform-specific driver
- replaces the existing vulnerable driver
- works across both x64 and ARM systems

This utility can be deployed across endpoints, and your MDM or vulnerability management tooling can be used to verify remediation status.

You can download the driver update utility here:
https://www.adminbyrequest.com/documents/ABRDriverUpdate.zip

On systems already running version 8.7 or later, the utility has no effect. It is safe to run repeatedly if needed.

Command line usage

To check whether the driver is updated:

```
ABRDriverUpdate.exe /P Action=Check
```

To update the driver:

```
ABRDriverUpdate.exe /P Action=Patch
```

Registry verification

In both cases, update status can be verified using the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\FastTrack Software\Admin By Request\DriverUpdated
```

If the driver has been successfully updated:

- **DriverUpdated** (REG_DWORD) will be set to **1**
- **DriverPatchTime** will contain the time of the update

If the utility is run again after the driver has already been updated, DriverPatchTime is not modified.

About the Patch Program

The patch program was built using FastTrack Automation Studio, available at:
https://www.fasttrackscript.com

FastTrack Automation Studio is developed by Admin By Request and can create self-contained executables from scripts. It is also suitable for building custom tray tools.

You can download the script source and patch utility here:
https://www.adminbyrequest.com/documents/ABRDriverUpdateScript.zip

This is provided in case you want to review or modify the script.

To build a self-contained executable in the script editor:

1. Select **Exe File > Advanced Exe File Compilation**
2. Choose **Include files from my project...** and include both driver files:
    - x64 driver
    - ARM driver