

beeware / briefcase Public[Code](#) [Issues](#) 164 [Pull requests](#) 17 [Discussions](#) [Actions](#) [Projects](#)

# Potential privilege escalation through MSI installers

High freakboy3742 published **GHSA-r3r2-35v9-v238** 2 weeks ago

## Package

 **briefcase** (pip)

### Affected versions

&gt;=0.3.0

### Patched versions

&gt;=0.3.26

## Description

### Impact

If a developer uses Briefcase to produce an Windows MSI installer for a project, and that project is installed for All Users (i.e., per-machine scope), the installation process creates a directory that inherits all the permissions of the parent directory. Depending on the location chosen by the installing user, this may allow a low privilege but authenticated user to replace or modify the binaries installed by the application. If an administrator then runs the altered binary, the binary will run with elevated privileges.

### Patches

The problem is caused by the template used to generate the WXS file for Windows projects. It was fixed with the following PRs:

- [beeware/briefcase-windows-app-template#86](#)
- [beeware/briefcase-windows-VisualStudio-template#85](#)

These patches have been backported to the templates used in Briefcase 0.3.26, 0.4.0, and 0.4.1. Re-running `briefcase create` on your Briefcase project will result in the updated templates being used.

### Workarounds

The change from [beeware/briefcase-windows-app-template#86](#) can be added to any existing Briefcase .wxs file generated by Briefcase 0.3.24 or later.

## References

[#2759](#) is a formal bug report of the problem.

### Severity

**High** 7.3 / 10

#### CVSS v3 base metrics

Attack vector	Local
Attack complexity	Low
Privileges required	Low
User interaction	Required
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

[Learn more about base metrics](#)

CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

### CVE ID

CVE-2026-33430

### Weaknesses

► CWE-732

### Credits

 Irandersson

Reporter