New issue

Privilege escalation with MSI installers #2759

Closed #2767

Labels bug windows

freakboy3742 opened 2 weeks ago Member

Describe the bug

Reported by **@lrandersson** via security@beeware.org.

MSI installers created with Briefcase do not set explicit permissions on the installation directory for per-machine (AllUsers) installs.
The directory inherits permissions from its parent, which can grant Authenticated Users write access to installed application files, enabling local privilege escalation.

Details

The WiX template at `{{ cookiecutter.format }}/{{ cookiecutter.app_name }}.wxs` does not configure any permission settings for the `INSTALLFOLDER` directory:

When the MSI installs with per-machine scope (ALLUSERS=1), the installation directory:

1. Does not have inheritance disabled (SE_DACL_PROTECTED flag is not set)
2. Inherits its DACL from the parent directory
3. May grant Authenticated Users modify/write permissions depending on the install location

This allows any authenticated user on the system to modify application executables and libraries, which can be exploited for privilege escalation if a higher-privileged user or service executes the application.

A similar vulnerability was identified and fixed in our NSIS-based installers:
https://nvd.nist.gov/vuln/detail/CVE-2022-26526.

How to reproduce the bug

1. Build an MSI installer using Briefcase with per-machine install scope
2. Install the MSI to a location outside of Program Files, such as C:\MyApp:

```
msiexec /i MyApp.msi ALLUSERS=1 INSTALLFOLDER="C:\MyApp"
```

3. Verify the inherited permissions using PowerShell:

```
Get-Acl -Path "C:\MyApp" | Format-List
```

4. Observe that:

- The SDDL contains D:AI (Auto-Inherited) instead of D:P (Protected)
- Authenticated Users have Modify permissions (0x1301bf)
- All ACEs have ID flags indicating inherited permissions

5. As a non-admin user, verify write access:

- echo test > "C:\MyApp\test.txt"

Minimum example code

```

```

Screenshots

No response

Environment details

- Operating system and version: Windows (tested on 10; but all versions)
- Python version: All
- Software versions:
  - Briefcase: 0.4.1 (but problem exists back to at least 0.3.0)

Logs

```

```

Additional context

Vulnerability type:

- Local Privilege Escalation (CWE-276: Incorrect Default Permissions)

Who is impacted:

- Users who install Briefcase-built MSI packages with per-machine scope
- Especially those who install to non-standard locations outside of Program Files
- Systems where multiple users share a machine

❤️ 1

freakboy3742 added bug windows 2 weeks ago

freakboy3742 mentioned this in 2 pull requests 2 weeks ago

- Ensure that MSIs installed for all users don't inherit permissions. briefcase-windows-app-template#86
- Ensure that MSIs installed for all users don't inherit permissions. briefcase-windows-VisualStudio-template#85

freakboy3742 2 weeks ago Member Author •••

The fix for this issue has been applied, and backported to the template branches for Briefcase v0.4.1, v0.4.0 and v0.3.26.

If you re-run `briefcase create` on any affected project with one of those versions of Briefcase, you should get an updated WXS file that will no longer have the privilege escalation issue.

We are awaiting allocation of a CVE by GitHub before making a formal security notification through Dependabot.

freakboy3742 mentioned this 2 weeks ago

- Add a release note for security issue. #2767

freakboy3742 closed this as completed in #2767 2 weeks ago

freakboy3742 2 weeks ago Member Author •••

The issue has been allocated CVE-2026-33430.

abdnh mentioned this 2 weeks ago

Update Briefcase's Windows template ankitects/anki#4630

Metadata

Assignees

No one assigned

Labels

bug windows

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with agent mode

Add a release note for security issue.

beeware/briefcase

Participants