2.43.7

Git v2.43.7 Release Notes ==========================

This release includes fixes for CVE-2025-27613, CVE-2025-27614, CVE-2025-46334, CVE-2025-46835, CVE-2025-48384, CVE-2025-48385, and CVE-2025-48386.

Fixes since v2.43.6 ------------------

- CVE-2025-27613, Gitk:

```
When a user clones an untrusted repository and runs Gitk without
additional command arguments, any writable file can be created and
truncated. The option "Support per-file encoding" must have been
enabled. The operation "Show origin of this line" is affected as
well, regardless of the option being enabled or not.
```

- CVE-2025-27614, Gitk:

```
A Git repository can be crafted in such a way that a user who has
cloned the repository can be tricked into running any script
supplied by the attacker by invoking `gitk filename`, where
`filename` has a particular structure.
```

- CVE-2025-46334, Git GUI (Windows only):

```
A malicious repository can ship versions of sh.exe or typical
textconv filter programs such as astextplain. On Windows, path
lookup can find such executables in the worktree. These programs
are invoked when the user selects "Git Bash" or "Browse Files" from
the menu.
```

- CVE-2025-46835, Git GUI:

```
When a user clones an untrusted repository and is tricked into
editing a file located in a maliciously named directory in the
repository, then Git GUI can create and overwrite any writable
file.
```

- CVE-2025-48384, Git:

```
When reading a config value, Git strips any trailing carriage
return and line feed (CRLF). When writing a config entry, values
with a trailing CR are not quoted, causing the CR to be lost when
the config is later read.  When initializing a submodule, if the
submodule path contains a trailing CR, the altered path is read
resulting in the submodule being checked out to an incorrect
location. If a symlink exists that points the altered path to the
submodule hooks directory, and the submodule contains an executable
post-checkout hook, the script may be unintentionally executed
after checkout.
```

- CVE-2025-48385, Git:

```
When cloning a repository Git knows to optionally fetch a bundle
advertised by the remote server, which allows the server-side to
offload parts of the clone to a CDN. The Git client does not
perform sufficient validation of the advertised bundles, which
allows the remote side to perform protocol injection.

This protocol injection can cause the client to write the fetched
bundle to a location controlled by the adversary. The fetched
content is fully controlled by the server, which can in the worst
case lead to arbitrary code execution.
```

- CVE-2025-48386, Git:

```
The wincred credential helper uses a static buffer (`target`) as a
unique key for storing and comparing against internal storage. This
credential helper does not properly bounds check the available
space remaining in the buffer before appending to it with
`wcsncat()`, leading to potential buffer overflows.
```

□□□ #2
□ □□□ □□□ 2026-10-31 20:02:42 UTC
□ □□□ □□□ 2026-10-31 20:02:43 UTC