New issue

VULN: Information Exposure Through Server Log Files #42

Open

BlackBird-BB opened 3 weeks ago

tufantunc ssh-mcp 1.5 Information Exposure Through Server Log Files

A local information exposure issue exists in ssh-mcp where SSH credentials are accepted via command-line (it is the only way to pass credentials) options (--password, --sudoPassword, --suPassword). Because process arguments are readable by unprivileged local users (via ps or /proc//cmdline on Linux, even low privilege), any attacker on the same host can directly recover plaintext passwords from the running process command-line string. This leads to credential leakage and violates secure handling of sensitive secrets in service startup parameters.

SSH Credentials Exposed via Command-Line Arguments

INFO

CWE: CWE-214 (Invocation of Non-Repudiable Function) / CWE-522 (Insufficiently Protected Credentials)

`--password`, `--sudoPassword`, `--suPassword` are passed as command-line arguments. And it is the **only** way to be passed to the server. Any local user(even **low privilege**) can read them via `ps aux`, `/proc/<pid>/cmdline`.

Location: `src/index.ts:6-16` (parseArgv), `src/index.ts:17-21`

Attack:

```
ps aux | grep ssh-mcp
# --password=MySecret --sudoPassword=SudoPass --suPassword=RootPass fully visible
```

Note: Reported separately in `ssh-mcp-credential-exposure.md`.

Valid

Terminal A: Start `ssh-mcp`, explicitly pass in the test password for observation, and confirm that the service process will run resident with these parameters.

Terminal B: Enumerate local processes in the same machine environment, directly read `/proc/<pid>/cmdline`, and confirm whether the plaintext credentials appear in the process command line.

Start `ssh-mcp` and pass in three types of test passwords in the startup parameters:

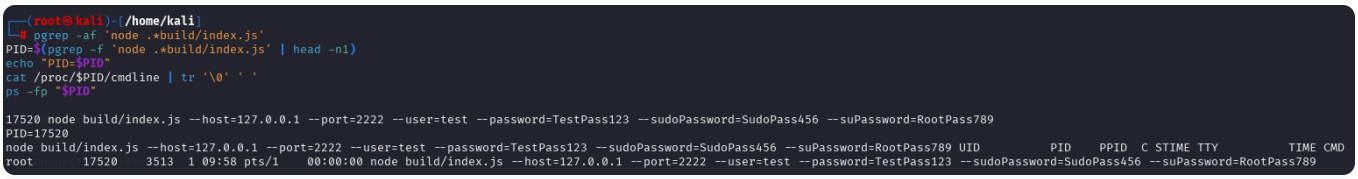
- `--password=TestPass123`
- `--sudoPassword=SudoPass456`
- `--suPassword=RootPass789`

```
cd /home/kali/ssh-mcp
node build/index.js \
  --host=127.0.0.1 \
  --port=2222 \
  --user=test \
  --password=TestPass123 \
  --sudoPassword=SudoPass456 \
  --suPassword=RootPass789
```

Check local process information on another terminal:

```
pgrep -af 'node .*build/index.js'
PID=$(pgrep -f 'node .*build/index.js' | head -n1)
echo "PID=$PID"
cat /proc/$PID/cmdline | tr '\0' ' '
ps -fp "$PID"
```

Observe that:




```
node build/index.js --host=127.0.0.1 --port=2222 --user=test --password=TestPass123 --
sudoPassword=SudoPass456 --suPassword=RootPass789
```

The same content can be directly read through `/proc/<pid>/cmdline`. It is not just possible to see the existence of the process, but also to directly read the complete plaintext parameters, including the SSH login password, `sudoPassword`, and `suPassword`.

As long as the service is started with passwords carried in command-line parameters, users on the same machine can directly read the plaintext credentials of SSH, `sudo`, and `su` through `ps` or `/proc/<<pid>/cmdline`.

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants