trifectatechfoundation / **sudo-rs** Public

Code Issues 67 Pull requests 8 Actions **Security** 5 Insight

Authenticating user not recorded properly in timestamp

Moderate **squell** published **GHSA-q428-6v73-fc4q** on Nov 11, 2025

Package

sudo-rs (Rust)

Affected versions	Patched versions
>0.2.5	0.2.10

Description

Summary

With `Defaults targetpw` (or `Defaults rootpw`) enabled, the password of the target account (or root account) instead of the invoking user is used for authentication. `sudo-rs` prior to 0.2.10 incorrectly recorded the invoking user's UID instead of the authenticated-as user's UID in the authentication timestamp. Any later `sudo` invocation on the same terminal while the timestamp was still valid would use that timestamp, potentially bypassing new authentication even if the policy would have required it.

Impact

A highly-privileged user (able to run commands as other users, or as root, through sudo) who knows one password of an account they are allowed to run commands as, would be able to run commands as any other account the policy permits them to run commands for, even if they don't know the password for those accounts.

A common instance of this would be that a user can still use their own password to run commands as root (the default behaviour of `sudo`), effectively negating the intended behaviour of the `targetpw` or `rootpw` options.

Example

With this in /etc/sudoers:

```
Defaults targetpw
user ALL=(ALL:ALL) ALL
```

First run:

```
user@machine$ sudo -g root whoami
[sudo: authenticate] Password: <password for user>
user
```

Then run:

```
user@machine$ sudo -u root whoami
root
```

Affected versions

sudo-rs prior to 0.2.5 are not affected, since they do not offer `Defaults targetpw` or `Defaults rootpw`.

Credits

This issue was discovered and reported by @Pingasmaster.

Severity

Moderate 4.4 / 10

CVSS v3 base metrics

Attack vector	Local
Attack complexity	Low
Privileges required	High
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	High
Availability	None

Learn more about base metrics

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

CVE ID

CVE-2025-64517

Weaknesses

▶ CWE-287

Improper Authentication

When an actor claims to have a given identity, the product does not prove or insufficiently proves that the claim is correct. Learn more on MITRE.

Credits

Pingasmaster	Reporter
bjorn3	Remediation developer
squell	Remediation reviewer