Team maintainer can transfer hosts from any team via missing source team authorization

High **lukeheath** published **GHSA-m2h6-4xpq-qw3m** 4 days ago

Package

github.com/fleetdm/fleet (Go)

Affected versions	Patched versions
< 4.81.1	>= 4.81.1

Description

Summary

A broken access control vulnerability in Fleet's host transfer API allows a team maintainer to transfer hosts from any team into their own team, bypassing team isolation boundaries. Once transferred, the attacker gains full control over the stolen hosts, including the ability to execute scripts with root privileges.

Impact

The host transfer endpoints verify that the caller has write permission to the destination team but do not check whether the caller has any permission over the source team of the hosts being transferred.

Once hosts are transferred, the attacker's team MDM configuration is automatically applied to the stolen devices, and the attacker can execute scripts on them with root privileges. In multi-tenant Fleet deployments where teams represent business units, departments, or customers, this breaks all team isolation guarantees. A bulk transfer variant allows stealing all matching hosts fleet-wide in a single request.

Exploitation requires authentication as a team maintainer or team admin.

Workarounds

There is no workaround for this issue short of upgrading to a patched version. Organizations concerned about exploitation should audit host transfer activity in their Fleet logs for any unexpected team reassignments.

For more information

If you have any questions or comments about this advisory:

Email us at security@fleetdm.com
Join #fleet in osquery Slack

Credits

We thank **@secfox-ai** for responsibly reporting this issue.

Severity

High

CVE ID

CVE-2026-29180

Weaknesses

No CWEs

Credits

prateek-0490 Analyst