Atlassian uses cookies to improve your browsing experience, perform analytics and research, and conduct advertising....
Atlassian cookies and tracking notice
✓ Accept all | Only necessary | Preferences

Grouper bug GRP-7359 - Grouper UI rules privilege escalation

By Chris Hyzer 7 min Add a reaction

Wiki Home	Grouper Release Announcements	Grouper Guides	Grouper Deployment Guide	Community Contributions

Grouper security vulnerability: privilege escalation via the rules UI

Publicly disclosed 2026/09/23. Fixed containers v7.5.1 (2026/09/26) and v6.4.1 (2026/09/27) are released. Until you upgrade, apply the mitigation below now.

Short version: In affected versions, a user who is allowed to create or edit rules in the User Interface can escalate privileges. **Assume this vulnerability is already known and could be exploited, and remediate as soon as possible** - do not wait for the fixed containers or an upgrade window. **Required action now: restrict rule creation in the UI to system administrators (the wheel group) with one**

Atlassian uses cookies to improve your browsing experience, perform analytics and research, and conduct advertising....
Atlassian cookies and tracking notice

1. the person can **authenticate to the Grouper UI**;

Updated Sept 30

configured, they are a **member of that group** (if it is not configured, this condition does not apply).

This vulnerability was discovered by Shilen Patel at Duke University.

Timeline

- 2026/09/23 public disclosure of the vulnerability and the configuration mitigation (exploit details / commit withheld until the fixed containers ship)
- 2026/09/26 fixed container v7.5.1 released (see v7 Release Notes)
- 2026/09/27 fixed container v6.4.1 released (see v6 Release Notes)
- 2026/09/30 CVE registration request: CAN-2026-2038636

Affected versions

The vulnerability is in the rules User Interface (the "Rules" screen on a group or folder), which was introduced in Grouper 5.8.3.

Release line	Affected
v2.6, v4 and earlier	No (no rules UI)
v5.0.0 - v5.8.2	No (before the rules UI)
v5.8.3 - v5.22.x	Yes (v5 is out of support; no v5 fix - upgrade)
v6.0.0 - v6.4.0	Yes
v6.4.1+	No (fixed)

Atlassian uses cookies to improve your browsing experience, perform analytics and research, and conduct advertising....
Atlassian cookies and tracking notice

Who is impacted

Updated Sept 30

allowed to create or edit rules in the UI. In practice this means the rules UI is reachable by non-sysadmins and `rules.restrictRulesUiToMembersOfThisGroupName` (in grouper.properties) is either blank or set to a group broader than your sysadmins.

- **Not impacted:** deployments where only Grouper sysadmins (wheel/root) can create or edit rules. A sysadmin authoring a rule that runs with elevated authority is not an escalation, since sysadmins are already fully privileged.

⚠ **Only the User Interface is affected.** Creating rules by any other path (Web Services, GSH/loader, or the MCP server) requires privileges that ordinary users do not have and is subject to the normal authorization checks, so those paths are not a vector.

What you should do now

The order matters: stop new rule creation first, then look at what already exists.

1. **Restrict the rules UI to system administrators (stop new exposure).** First find the name of your system administrators (wheel) group - it is the value of the `groups.wheel.group` property in grouper.properties (the stem prefix is site-specific, so do not assume it is under `etc:`). Then set the property below in grouper.properties to that group name, in every environment (dev/test/prod/etc):

```
# grouper.properties  (use YOUR sysadmin group - the value of g
rules.restrictRulesUiToMembersOfThisGroupName = your:sysadmin:g
```

Atlassian uses cookies to improve your browsing experience, perform analytics and research, and conduct advertising....
Atlassian cookies and tracking notice

minutes for it to take effect (the rules-editor cache is 5 minutes and the wheel-member cache adds a few more) - or restart Grouper to apply it

Updated Sept 30

2. **Audit existing rules.** Restricting the UI does not remove rules that were already created. Run the read-only report (, attached to this page) to find rules that may have been created by someone who should not have been able to. See "Auditing existing rules" below for how to read it.
3. **Clean up.** Remove any rule that should not be there.

Remediation methods

The configuration restriction above is the immediate mitigation. Upgrading is the permanent fix that lets you safely re-open rule authoring to non-sysadmins.

Remediation method 1: restrict the rules UI (configuration, immediate)

The configuration change under "What you should do now". No code, takes effect after a cache clear or restart. Apply it in all environments (dev/test/prod/etc). This confines rule authoring to system administrators (the wheel group) until you upgrade. Keep it in place until then.

There is no separate on/off switch for the rules UI; restricting it to the wheel group (system administrators) is the supported way to close it. Related properties (also in grouper.properties) `rules.groupNamesRestrictRules` and `rules.stemNamesRestrictRules` tighten things somewhat but are not a substitute for this restriction.

Remediation method 2: upgrade Grouper

Grouper v7.5.1+ (released 2026/09/26) and v6.4.1+ (released 2026/09/27) fix this vulnerability. These are patch releases that also carry a Tomcat security upgrade (v7.5.1 also has two small container fixes; see v7 Release Notes), and

Atlassian uses cookies to improve your browsing experience, perform analytics and research, and conduct advertising....
Atlassian cookies and tracking notice

upgrade to a supported release. After upgrading you can widen `rules.restrictRulesUiToMembersOfThisGroupName` (in grouper.properties)

Updated Sept 30

Behavior changes in the fixed versions:

- Non-sysadmins can only create or edit rules from the predefined patterns, and the rule must match the selected pattern. Custom rules and rules that use expression language (EL) are sysadmin-only.
- Rules that send email: if `rules.restrictRulesEmailSendersToMembersOfThisGroupName` is set, only its members (and sysadmins) can create them; otherwise members of the `rules.restrictRulesUiToMembersOfThisGroupName` group can. If neither is set, only sysadmins can, unless you set `rules.allowSendEmailRulesWhenNoGroupConfigured = true`.
- We recommend keeping `rules.restrictRulesUiToMembersOfThisGroupName` set to a group of trusted power users rather than leaving it blank. See Grouper rules UI.

Remediation method 3: patch the container

No binary patches are planned for this issue. The vulnerability can be fully mitigated by the configuration restriction (method 1), and supported deployments should stay current by upgrading (method 2). If a need arises, patches can be produced in the future; contact Chris Hyzer (Internet2 Slack).

How to test the remediation

You can verify the restriction without a second account, using your own, by temporarily making yourself a non-sysadmin who still has ADMIN on the sysadmin group so you can manage it:

1. Confirm `rules.restrictRulesUiToMembersOfThisGroupName` is set to your sysadmin (wheel) group and is in effect.

Atlassian uses cookies to improve your browsing experience, perform analytics and research, and conduct advertising....
Atlassian cookies and tracking notice

4. Wait for the caches to clear - up to about 10 minutes (rules-editor cache 5

Updated Sept 30

5. View rules on the sysadmin group. You should see **no "Add rule" button** (you have ADMIN, but you are no longer a member of the restrict group), which confirms the restriction is working.
6. **Clean up:** add yourself back as a member of the sysadmin group, then remove the direct ADMIN privilege you granted yourself in step 2.

Auditing existing rules (interpreting ruleSecurityReport.gsh)

This page has `_` attached - a read-only command-line GSH report (work in progress; heuristics still being tuned). Download it from the attachment, run it, and capture the output:

```
[tomcat@serverName bin]$ ./gsh.sh ruleSecurityReport.gsh > /tmp/ru
```

Run it from the Grouper container's `WEB-INF/bin` directory as the `tomcat` user (the same account Grouper runs as), so it has the container's classpath and DB config.

Step by step (for example, inside the container/host shell):

1. Become the tomcat user: `sudo -u tomcat bash`
2. Go to the bin directory (adjust the path if your container differs): `cd /opt/grouper/grouperWebapp/WEB-INF/bin`
3. Create the file: `vi ruleSecurityReport.gsh`, press `i` to insert, paste the full contents of the attached `_`, press `ESC`, then type `:wq` and Enter to save.
4. Run it, sending the output to a file under `/tmp`: `./gsh.sh ruleSecurityReport.gsh > /tmp/ruleSecurityReport.out.txt 2>&1` (if `/tmp` is not writable in your environment, just drop the `>`

Atlassian uses cookies to improve your browsing experience, perform analytics and research, and conduct advertising....
Atlassian cookies and tracking notice

summary.

Updated Sept 30

privileges (whether that person was in the wheel group, or held the required UPDATE/ADMIN/STEM_ADMIN, *at the time of the edit*). A rule is OK if it was created by GrouperSystem/root, by a wheel member at the time, by someone who held the needed privilege at the time, or by any path other than the rules UI (Web Services, GSH/loader, or inside a GSH template run) - since the vulnerability is UI-only and those paths require ATTR_UPDATE on the rule attributeDefs, which non-sysadmins do not have.

To cut noise it skips rules last edited before the vulnerable UI first shipped (2024-03-03; a one-line cutoff you can tighten to your own deploy date), allows a short tolerance on the privilege check (a folder rule is usually created in the same batch as its folder and grant), and prints only the flagged rules in two clearly divided, numbered sections:

- **SECTION 1 - FLAG-OTHER**: non-inherited pattern; **review these first.**
- **SECTION 2 - FLAG-INHERITED**: inherited-privilege pattern. **Most of these are false positives.** They are shown so a real one cannot slip through, but expect the large majority to be legitimate - for example a rule assigned by a GSH template can look inappropriate (the person who ran the template does not personally hold the folder privilege) yet is entirely correct, because the template is a trusted operation.

It ends with a summary (total / skipped / evaluated / OK / flagged-other / flagged-inherited). **Treat verdicts as guidance, not proof:** OK is not proof of safe and FLAG is not proof of malicious. This report relies on the audit log and point-in-time (PIT) data, and **neither is authoritative** - both are cleaned up / purged on a retention schedule and can be altered, so history may be missing or changed. On top of that the "who" is best effort: audit can be suppressed for some attribute defs, purged by retention (such rules show "authorship

Atlassian uses cookies to improve your browsing experience, perform analytics and research, and conduct advertising....
Atlassian cookies and tracking notice

report.

Updated Sept 30

Prepared for Grouper administrators. Questions: Chris Hyzer (Internet2 Slack). Publicly disclosed 2026/09/23; v7.5.1 released 2026/09/26; v6.4.1 released 2026/09/27.

Add a comment

Add a reaction