

Grouper Security Issues

Wiki Home	Grouper Release Announcements	Grouper Guides	Grouper Deployment Guide	Community Contributions	Internal Developer Resources
---------------------------	---	--------------------------------	--	---	--

This page provides access to the complete history of Security Advisories released for Grouper and an "at a glance" table showing you which releases are vulnerable to what kinds of issues. If you're running a particular version, you can use this table to identify the issues that could affect your system and determine how urgent an upgrade is. In addition to the [announce](#) mailing list, you can "watch" this page for changes to keep abreast.

You can determine the exact version you're running based on the process log during startup.

If you would like to report an issue you believe is security related, you can:

- e-mail [grouper core](#)

As always, sites are advised to use the latest stable release of any Grouper product. Refer to the [Grouper Downloads](#) page for information about our support and versioning policies. The [Security Advisories](#) page identifies the specific versions recommended at a given point in time

Obviously not all vulnerabilities are created equal, and the classifications in the matrices are general in nature, and are meant to point you to the relevant advisories to look into.

A particular version will typically be implicated by any advisories noted for it and for any newer versions above it in the tables.

Advisories noted for "All" versions should be reviewed by all deployers for relevancy to their deployment. Typically this indicates that an advisory is at least partly discussing issues that go beyond the scope of what the Grouper software can actually remediate and may affect the deployment as a whole. It does not in general refer to unfixed vulnerabilities in the Grouper software itself.

Security Issues

Date fixed	Affects versions	Fixed in versions	Jira	Description
3-Nov-2023	2.5.23-2.5.68, v2.6.0-v2.6.19, v4.0.1-v4.7.2, v5.0.3-v5.4.0	v2.5.69, v4.8.0, v5.5.0	GRP-5107	Authentication bypass security issue
9-Nov-2020	2.5.36 and 2.5.37	2.5.36.1, 2.5.37.1, 2.5.38+	GRP-3015	container prints env vars to logs which can be passwords
14-May-2020	2.4 ui patch 46+, 2.5 up to 2.5.27	2.5.28	GRP-2705	Some encrypted values can be shown on UI to admins
24-Apr-2019	2.4	v2_4_0_api_patch_42	GRP-2110	Use SSL context while making rabbitmq connection
20-Aug-2018	2.3 ui patch 44	Patch for 2.3.0	GRP-1875	subject audits should only be seen by grouper admins
20-Aug-2018	2.3 api patch 109	Patch for 2.3.0	GRP-1876	flash cache in groups can allow subjects to view (not read) objects with quick subsequent requests
20-Jul-2018	2.2 and 2.3	Patch for 2.2.2 and 2.3.0	GRP-1838	xsrf problem with /UiV2Public.index
29-Nov-2015	1.4-2.2.2	Patch for 2.2.2	GRP-1227	security issue with subject api init params
18-Nov-2015	2.2.0, 2.2.1, 2.2.2	Patch for 2.2.2	GRP-1222	xss vulnerability in tooltips in new UI
14-Sep-2013	2.1.5 and before		GRP-934	Grouper UI is susceptible to CSRF / XSRF Cross site request forgery
16-Aug-2013	1.4, 1.5, 1.6, 2.0, 2.1 (build 0,1,2,3,4)	1.4.2, 1.5.3, 1.6.3, 2.0.3, 2.1.4	GRP-928	Grouper UI allows unauthorized users to view the privileges of other subjects
2-Aug-2013	1.6, 2.0, 2.1 (build 0,1,2,3)	1.6.3, 2.0.3, 2.1.3	GRP-880	Deleting an attributeDef can cause incorrect membership deletes
1-Aug-2013	1.6, 2.0, 2.1 (build 0,1,2,3,4)	1.6.3, 2.0.3, 2.1.4	GRP-911 and GRP-924	Unauthorized users can delete attribute assignments

28-Jul-2013	1.4, 1.5, 1.6, 2.0, 2.1 (build 0,1,2,3,4)	1.4.2, 1.5.3, 1.6.3, 2.0.3, 2.1.4	GRP-923	WS getGrouperPrivilegesLite can return more data than the user should be able to see
22-Dec-2010	1.5 (build 0,1,2,3), 1.6 (build 0,1,2)	1.5.3, 1.6.2	GRP-519	A bug in the Grouper UI allows unauthorized users to view user audit logs by URL manipulation

- [Grouper Bug GRP-880](#) - Deleting an attributeDef can cause incorrect membership deletes
- [Grouper Bug GRP-911 and GRP-924](#) - Unauthorized users can delete attribute assignments
- [Grouper Bug GRP-923](#) WS getGrouperPrivilegesLite can return more data than the user should be able to see
- [Grouper Bug GRP-928](#) - Grouper UI allows unauthorized users to view the privileges of other subjects
- [Grouper bug - GRP-5107](#) - authentication bypass
- [GRP 519](#) - A bug in the Grouper UI allows unauthorized users to view user audit logs by URL manipulation

See Also

[Grouper Versioning and Support Policy](#) for earlier Grouper releases.

[Grouper Security Issue Reporting](#)

[Externalize and encrypt grouper passwords morphString morph](#)