



# CVE-2018-12423

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2018-12423
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-06-14 21:29:00 UTC
<b>Updated</b>	2019-10-03 00:03:00 UTC
<b>Description</b>	In Synapse before 0.31.2, unauthorised users can hijack rooms when there is no m.room.power_levels event in force.

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Matrix</a>	<a href="#">Synapse</a>	All	All	All	All
Application	<a href="#">Matrix</a>	<a href="#">Synapse</a>	All	All	All	All

## References

### Reference

- [Proposal to simplify the auth rules of m.room.power\\_level events. · Issue #1304 · matrix-org/matrix-doc · GitHub](#)
- [#901549 - matrix-synapse: CVE-2018-12423: unauthorised users can hijack rooms when there is no m.room.power\\_levels event in force - Del](#)
- [Security update: Synapse 0.31.2 | Matrix.org](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[199533](#) [Ubuntu Security Notification for Synapse Vulnerabilities \(USN-6076-1\)](#)

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**