

SAML Single Sign On (by resolution) - 2021-07-29

Communication by Vendor

Summary

This advisory discloses a **critical severity** security vulnerability affecting our SAML Single Sign-On Plugin in all past versions.

Please **upgrade your** installations to fix this vulnerability.

Details

The security vulnerability has been made known to us via disclosure from a researcher. To our knowledge, this is currently not otherwise known or widely exploited.

Due to the severe nature of this vulnerability, we will not currently provide detailed information that may increase the risk of it being exploited. We will first allow a time window that customers should utilize to upgrade to the fixed versions.

Nevertheless, there is an imperfect way to detect whether this vulnerability was exploited on your instance. For information on how to do this, please contact us with your valid, non-evaluation app SEN via our [Support Portal](#)

What You Need to Do

In general, **please update the SAML SSO app to the latest versions.** For information about how to update your apps, please refer to [Atlassian's documentation](#) on the topic

If you **cannot** update the app, the only way to get rid of this vulnerability is to disable the app. Note that this will result in loss of Single Sign-On capability for all users on the effected system.

You might be able to mitigate the impact by restricting access to the product from the internet to only your known users using an internal VPN or a similarly private network. Note that this requires you to trust your users not to exploit this vulnerability.

The updated versions of the app make the fix available for all currently supported versions of the Atlassian host products (Jira, Confluence, Bitbucket, Bamboo, Fisheye/Crucible). If you require a fixed app version for unsupported Atlassian host products that do not work with one of the provided versions, please raise a support request via our [Support Portal](#).

If you need help with either of these courses of action, please raise a support request via our [Support Portal](#).

Support

If you have questions or concerns regarding this advisory, please raise a support request via our [Support Portal](#).

Fixed App Versions By Host Product Versions

This table denotes which host product versions are compatible with which app versions (Atlassian Application SAML SSO app version).

- **Jira**
 - 7.3.0 - 8.14.1 3.6.6.1
 - 7.13.0 - 8.17.0 4.0.12
 - 8.3.0 - 8.18.1 5.0.5
- **Confluence**
 - 6.0.1 - 7.8.3 3.6.6
 - 6.13.0 - 7.12.3 4.0.12
 - 7.0.1 - 7.12.3 5.0.5
- **Bitbucket**
 - 5.5.0 - 6.10.2 2.5.9
 - 5.12.4 - 7.15.0 3.6.6

Date	29 Jul 2021
Product	SAML Single Sign On
Vulnerability	Critical
Marketplace link	https://marketplace.atlassian.com/apps/1212130/ https://marketplace.atlassian.com/apps/1212129/ https://marketplace.atlassian.com/apps/1217045/ https://marketplace.atlassian.com/apps/1217672/ https://marketplace.atlassian.com/apps/1219441/
Base product	Jira, Confluence, Bitbucket, Bamboo, Fisheye
Vendor	resolution Reichert Network Solutions GmbH

- 6.0.0 - 7.15.0 4.0.12
 - 6.4.0 - 7.15.0 5.0.5
- *Bamboo*
 - 5.12.0.2 - 6.10.6 2.5.9
 - 6.6.0 - 7.1.4 3.6.6
 - 6.8.0 - 7.2.5 4.0.12
 - 6.10.2 - 7.2.5 5.0.5
- *Fisheye/Crucible*
 - 4.2.0 - 4.8.7 2.5.9

For example, if you use Bamboo 6.6.0 with SAML SSO app version 2.5.5, you can update to 2.5.9 or 3.6.6

Recommendation by bitvoodoo

- Upgrade the app to the appropriate version

If you need any assistance please contact our Support Team.