Questions For Confluence Security Advisory 2022-07-20

Update: This advisory has been updated since its original publication.

01 Aug 2022 12:00 PM PDT (Pacific Time, -7 hours)

- Updated the *Fixes* section to note that if the `disabledsystemuser` account is manually deleted, the app must also be updated or uninstalled to ensure the account does not get recreated

01 Aug 2022 11:00 AM PDT (Pacific Time, -7 hours)

- Updated the *Summary of Vulnerability* section to note the email service provider for the `dontdeletethisuser@email.com` account has confirmed the account has been blocked

30 Jul 2022 12:30 PM PDT (Pacific Time, -7 hours)

- Updated the *Summary of Vulnerability* and *Severity* sections to note that instances that have not remediated this vulnerability per the *Fixes* section may send email notifications from Confluence to a third party email address
- Added a new section *How To Look For Evidence of Information Disclosure Via Email*

22 Jul 2022 9:30 AM PDT (Pacific Time, -7 hours)

- Updated the *Fixes* section to explain only option 2 can be used for Confluence Server and Data Center instances configured to use a read-only external directory

22 Jul 2022 9:00 AM PDT (Pacific Time, -7 hours)

- Added a link to a page of frequently asked questions about CVE-2022-26138

21 Jul 2022 8:30 AM PDT (Pacific Time, -7 hours)

- An external party has discovered and publicly disclosed the hardcoded password on Twitter. **It is important to remediate this vulnerability on affected systems immediately.**
- The *Summary of Vulnerability* and *Severity* sections have been updated to include this new information

Summary	Confluence account with hardcoded credentials created by Questions for Confluence
Advisory Release Date	20 Jul 2022 10:00 AM PDT (Pacific Time, -7 hours)
Affected Products	Questions For Confluence app for:

	• Confluence Server • Confluence Data Center ℹ The Questions for Confluence app for Confluence Cloud is not affected.
CVE ID(s)	CVE-2022-26138

Summary of Vulnerability

When the Questions for Confluence app is enabled on Confluence Server or Data Center, it creates a Confluence user account with the username `disabledsystemuser`. This account is intended to aid administrators that are migrating data from the app to Confluence Cloud. The `disabledsystemuser` account is created with a hardcoded password and is added to the `confluence-users` group, which allows viewing and editing all non-restricted pages within Confluence by default. A remote, unauthenticated attacker with knowledge of the hardcoded password could exploit this to log into Confluence and access any pages the `confluence-users` group has access to.

The `disabledsystemuser` account is configured with a third party email address (`dontdeletethisuser@email.com`) that is not controlled by Atlassian. If this vulnerability has not been remediated per the *Fixes* section below, an affected instance configured to send notifications will email that address. One example of an email notification is Recommended Updates Notifications, which contains a report of the top pages from Confluence spaces the user has permissions to view. mail.com, the free email provider that manages the `dontdeletethisuser@email.com` account, has confirmed to Atlassian that the account has been blocked. This means it cannot be accessed by anyone unauthorized and cannot send or receive any new messages.

An external party has discovered and publicly disclosed the hardcoded password on Twitter. Refer to the *Fixes* section below for guidance on how to remediate this vulnerability.

Severity

⚠ This vulnerability should be remediated on affected systems immediately for the following reasons:

- The hardcoded password is publicly known
- There are reports of this vulnerability being exploited in the wild
- Instances where this vulnerability has not been remediated per the *Fixes* section below may be configured to send email notifications from Confluence to a third party email address that is not controlled by Atlassian

Atlassian rates the severity level of this vulnerability as **critical**. The scale allows us to rank the severity as critical, high, moderate or low. This is our assessment, and you should evaluate its applicability to your own IT environment.

How To Determine If You Are Affected

A Confluence Server or Data Center instance is affected if it has an active user account with the following information:

- User: `disabledsystemuser`
- Username: `disabledsystemuser`
- Email: `dontdeletethisuser@email.com`

⚠️ It is possible for this account to be present if the Questions for Confluence app has previously been installed and uninstalled.

If this account does not show up in the list of active users, the Confluence instance is not affected.

Affected Versions

⚠️ These are the versions of the app that create the `disabledsystemuser` account with a hardcoded password. Confluence installations that do not actively have any of these versions of the app installed **may still be affected**. Refer to the *How To Determine If You Are Affected* section above and the *Remediation* section below for more information.

Questions for Confluence 2.7.x	• 2.7.34 • 2.7.35
Questions for Confluence 3.0.x	• 3.0.2

Fixes

Uninstalling the Questions for Confluence app does **not** remediate this vulnerability. The `disabledsystemuser` account does not automatically get removed after the app has been uninstalled. If you have verified a Confluence Server or Data Center instance is affected, two equally effective ways to remediate this vulnerability are listed below.

These options either disable or remove the `disabledsystemuser` account. Configuring data migration from the app to Confluence Cloud is now a manual process.

Option 1: Update to a non-vulnerable version of Questions for Confluence

Update the Questions for Confluence app to a fixed version:

- 2.7.x >= 2.7.38 (compatible with Confluence 6.13.18 through 7.16.2)
- Versions >= 3.0.5 (compatible with Confluence 7.16.3 and later)

For more information on how to update an app, refer to:

https://confluence.atlassian.com/upm/updating-apps-273875710.html

Fixed versions of the Questions for Confluence app stop creating the `disabledsystemuser` user account, and remove it from the system if it has already been created.

> ⚠ If Confluence is configured to use a read-only external directory (e.g. Atlassian Crowd), you will need to follow Option 2 below.

Option 2: Disable or delete the `disabledsystemuser` account

Search for the `disabledsystemuser` account and either disable it or delete it. For instructions on how to disable or delete an account (including an explanation of the differences between the two options), refer to:

https://confluence.atlassian.com/doc/delete-or-disable-users-138318.html

If you choose to delete the `disabledsystemuser` account, you must also uninstall or upgrade the Questions for Confluence app to a non-vulnerable version. **Failure to do this could result in the account being recreated after it has been deleted.**

If Confluence is configured to use a read-only external directory, refer to the *Delete from a read-only external directory, or multiple external directories* section of the same document:

https://confluence.atlassian.com/doc/delete-or-disable-users-138318.html#DeleteorDisableUsers-Deletefromaread-onlyexternaldirectory,ormultipleexternaldirectories

How To Look For Evidence of Exploitation

To determine if anyone has successfully logged in to the `disabledsystemuser` account, refer to the following document which provides instructions on how to get a list of users' last logon times:

https://confluence.atlassian.com/confkb/how-to-get-a-list-of-users-with-their-last-logon-times-985499701.html

If the last authentication time for `disabledsystemuser` is `null`, that means the account exists but no one has ever logged into it.

How To Look For Evidence of Information Disclosure Via Email

To determine if Confluence has sent any email notifications to a third party email account, review the logs of the SMTP server configured to send outbound mail from Confluence for any messages sent to the address `dontdeletethisuser@email.com`

Frequently Asked Questions

We'll update the FAQ for CVE-2022-26138 with answers for commonly asked questions.

Related Tickets

- CONFSERVER-79483 - Getting issue details... STATUS

Support

If you did not receive an email for this advisory and you wish to receive such emails in the future, go to https://my.atlassian.com/email and subscribe to Alerts emails.

If you have questions or concerns regarding this advisory that aren't answered in the FAQ, please raise a support request at https://support.atlassian.com/.

References

Security Bug fix Policy	As per our new policy, critical security bug fixes will be back ported in accordance with https://www.atlassian.com/trust/security/bug-fix-policy . We will release new maintenance releases for the versions covered by the policy instead of binary patches. **Binary patches are no longer released.**
Severity Levels for security issues	Atlassian security advisories include a severity level and a CVE identifier. This severity level is based on our self-calculated CVSS score for each specific vulnerability. CVSS is an industry standard vulnerability metric. You can learn more about CVSS at FIRST.org.
End of Life Policy	Our end of life policy varies for different products. Please refer to our EOL Policy for details.

Last modified on Aug 4, 2022