CERT-EU

Security Advisory 2022-052

Critical Vulnerability in *Questions for Confluence*

August 01, 2022 — v1.1

TLP:WHITE

History:

- *22/07/2022 — v1.0 – Initial publication*
- *01/08/2022 — v1.1 – Update on information disclosure to third party and how to detect it*

Summary

On July 20th, Atlassian released a security advisory to address a critical vulnerability that affects the *Questions for Confluence* app [1]. Having the app enabled on Confluence Server or Data Center, it creates the Confluence user account `disabledsystemuser`. The account is is intended to aid administrators, and it 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 [2]. 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.

[UPDATE] The `disabledsystemuser` account is configured with a third party email address that is not controlled by Atlassian, meaning that an affected instance configured to send notifications [3], will e-mail that address and potentially disclosing information.

The hardcoded password was publicly disclosed by an external party in Twitter [4] on July 21st, which makes the exploitation in the wild highly likely, therefore immediate update to a patched version is highly recommended.

Technical Details

How to Determine if You Are Affected

Admins who want to determine if their Confluence Server or Data Center instance is affected, have to check for an active user account with the following information:

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

If the account is not in the list of active users, the Confluence instance is not affected.

Please note, it is possible for this account to exist even if the *Questions for Confluence* app has been previously installed and uninstalled.

How to Look for Evidence of Exploitation

To determine if the vulnerability has been exploited, you can consult Confluence documentation on how to get a list of users with their last logon times. If the last authentication time for `disabledsystemuser` is `null`, that means the account exists, but no one has ever logged into it.

Please find the link to the documentation at the bottom of the page [5].

[UPDATE] How To Look For Evidence of Information Disclosure Via Email

In order to determine if Confluence has sent e-mail notifications to third party e-mails, Atlassian suggests to review the logs of the SMTP server configured to send outbound mail from Confluence [6] and identify any messages sent to the `dontdeletethisuser@email.com` address.

Affected Products

The following products are affected by the vulnerability:

- Questions for Confluence 2.7.x - versions 2.7.34, 2.7.35
- Questions for Confluence 3.0.2 - version 3.0.2

Please be aware that these are the versions of the app that create the `disabledsystemuser` user with a hardcoded password, however, 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 for more information.

Recommendations

The following two options have been provided to address the flaw:

- **Update to a non-vulnerable version of Questions for Confluence:**
  - For versions 2.7.x, update to 2.7.38 or higher.
  - Version 3.0.5 or higher.
- **Disable or delete the disabledsystemuser account.**

Please note that uninstalling the *Questions for Confluence* app does not remediate this vulnerability, as the `disabledsystemuser` account does not automatically get removed after the app has been uninstalled.

References

[1] https://confluence.atlassian.com/doc/questions-for-confluence-security-advisory-2022-07-20-1142446709.html

[2] https://confluence.atlassian.com/doc/confluence-groups-139478.html

[3] https://confluence.atlassian.com/doc/email-notifications-145162.html

[4] https://twitter.com/fluepke/status/1549892089181257729

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

[6] https://confluence.atlassian.com/doc/configuring-a-server-for-outgoing-mail-151078.html