Hardcoded password in Confluence app has been leaked on Twitter

Getty Images

reader comments

63 with 43 posters participating

Share this story

What’s worse than a widely used Internet-connected enterprise app with a hardcoded password? Try said enterprise app after the hardcoded password has been leaked to the world.

Atlassian on Wednesday revealed three critical product vulnerabilities, including CVE-2022-26138 stemming from a

hardcoded password in Questions for Confluence, an app that allows users to quickly receive support for common questions involving Atlassian products. The company warned the passcode was “trivial to obtain.”

The company said that Questions for Confluence had 8,055 installations at the time of publication. When installed, the app creates a Confluence user account named disabledsystemuser, which is intended to help admins move data between the app and the Confluence Cloud service. The hardcoded password protecting this account allows for viewing and editing of all non-restricted pages within Confluence.

“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 company said. “It is important to remediate this vulnerability on affected systems immediately.”

A day later, Atlassian was back to report that “an external party has discovered and publicly disclosed the hardcoded password on Twitter,” leading the company to ratchet up its warnings.

“This issue is likely to be exploited in the wild now that the hardcoded password is publicly known,” the updated advisory read. “This vulnerability should be remediated on affected systems immediately.”

The company warned that even when Confluence installations don’t actively have the app installed, they may still be vulnerable. Uninstalling the app doesn’t automatically remediate the vulnerability because the disabledsystemuser account can still reside on the system.

To figure out if a system is vulnerable, Atlassian advised Confluence users to search for accounts with the following information:

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

Atlassian provided more instructions for locating such accounts here. The vulnerability affects Questions for Confluence versions 2.7.x and 3.0.x. Atlassian provided two ways for customers to fix the issue: disable or remove the "disabledsystemuser" account. The company has also published this list of answers to frequently asked questions.

Confluence users looking for exploitation evidence can check the last authentication time for disabledsystemuser using the instructions here. If the result is null, the account exists on the system, but no one has yet signed in using it. The commands also show any recent login attempts that were successful or unsuccessful.

"Now that the patches are out, one can expect patch diff and reversing engineering efforts to produce a public POC in a fairly short time," Casey Ellis, founder of vulnerability reporting service Bugcrowd, wrote in a direct message. "Atlassian shops should get on to patching public-facing products immediately, and those behind the firewall as quickly as possible. The comments in the advisory recommending against proxy filtering as mitigation suggest that there are multiple trigger pathways.

The other two vulnerabilities Atlassian disclosed on Wednesday are also serious, affecting the following products:

- Bamboo Server and Data Center
- Bitbucket Server and Data Center
- Confluence Server and Data Center
- Crowd Server and Data Center
- Crucible
- Fisheye
- Jira Server and Data Center

- Jira Service Management Server and Data Center

Tracked as CVE-2022-26136 and CVE-2022-26137, these vulnerabilities make it possible for remote, unauthenticated hackers to bypass Servlet Filters used by first- and third-party apps.

“The impact depends on which filters are used by each app, and how the filters are used,” the company said. “Atlassian has released updates that fix the root cause of this vulnerability but has not exhaustively enumerated all potential consequences of this vulnerability.”

Vulnerable Confluence servers have long been a favorite opening for hackers looking to install ransomware, cryptominers, and other forms of malware. The vulnerabilities Atlassian disclosed this week are serious enough that admins should prioritize a thorough review of their systems, ideally before the weekend starts.

https://arstechnica.com/?p=1868878