Cloudflare server breached using old credentials from previous attack

Cloud cyber security company Cloudflare has revealed that a "nation-state" threat actor has breached its internal Atlassian server.

Daniel Croft

• Fri, 02 Feb 2024 • **SECURITY**

According to a company blog post, the attack first accessed Cloudflare's systems for reconnaissance from 14 to 17 November and accessed a number of systems, including the company's "internal wiki (which uses Atlassian Confluence) and our bug database (Atlassian Jira)".

The attackers reportedly returned days later on 20 and 21 November, likely to verify that they still had a connection.

"They then returned on November 22 and established persistent access to our Atlassian server using ScriptRunner for Jira, gained access to our source code management system (which uses Atlassian Bitbucket), and tried, unsuccessfully, to access a console server that had access to the data centre that Cloudflare had not yet put into production in São Paulo, Brazil," the company added.

"Analysing the wiki pages they accessed, bug database issues, and source code repositories, it appears they were looking for information about the architecture, security, and management of our global network; no doubt with an eye on gaining a deeper foothold."

The attacker reportedly accessed the systems using an access token and a trio of service account credentials that were obtained during the Okta breach that affected Cloudflare in October 2023.

Cloudflare said that it failed to rotate those connections but that as of 24 November, all connections that the threat actor had made were terminated.

It also has confirmed with CrowdStrike that there is no new evidence of threat activity since.

“Even though we understand the operational impact of the incident to be extremely limited, we took this incident very seriously because a threat actor had used stolen credentials to get access to our Atlassian server and accessed some documentation and a limited amount of source code,” added Cloudflare.

“Based on our collaboration with colleagues in the industry and government, we believe that this attack was performed by a nation-state attacker with the goal of obtaining persistent and widespread access to Cloudflare’s global network.”

Following the breach, Cloudflare has begun bolstering its systems in a project it has called “Code Red”, which focuses on investigating its systems and “strengthening, validating and remediating any control in our environment to ensure we are secure against future intrusion and to validate that the threat actor could not gain access to our environment”.

Code Red ended on 5 January, but the company has continued to monitor its systems and strengthen its security.

The Okta breach that led to the most recent incident occurred on 18 October last year, leading to a threat actor accessing credentials, all of which were meant to be rotated. However, Cloudflare failed to rotate a single service token and three service accounts, which were used in the most recent breach.

“The one service token and three accounts were not rotated because mistakenly it was believed they were unused,” the company said.

“This was incorrect and was how the threat actor first got into our systems and gained persistence to our Atlassian products.

“Note that this was in no way an error on the part of AWS, Moveworks or Smartsheet. These were merely credentials which we failed to rotate.”

COMMENTS (0)

Leave a comment

Comments powered by CComment