Kodi February 2023 Data Breach

Incident Name	Kodi February 2023 Data Breach
Date of Public Report	**April 8th, 2023**
Date of Incident	February 16th and 21st, 2023
Summary	Kodi is an open-source media player software provider created by the non-profit XBMC Foundation. On April 8th, 2023, Kodi disclosed a data breach in which the company confirmed a data dump of its MyBB forum database that was being advertised for sale online. The threat actor responsible was advertising data of 400,000 Kodi users on well-known breach forums. Kodi reported that the actor gained access by using a privileged account of an inactive member of the forum's admin team, which was accessed on February 16th and 21st. The company stated that this account was used by the hacker to create database backups which were then downloaded and deleted. The actor also downloaded existing night backups of the database. The data in the backups included public forum posts, team forum posts, and user data such as email addresses and encrypted passwords. The Kodi team, in response to this incident, has deactivated the compromised admin account and is reviewing the team's privileges. The company is also looking into how it can perform a global password reset and has taken the forum down while it determines the safest way to do this. Kodi has advised its forum users that they should consider their account as compromised and change their passwords elsewhere if they use the same username and password.
April 11th Update	As of April 11th, the Kodi team is working to bring the forum back online and has confirmed it has not seen any other evidence of compromise. In the process of deploying the new forum, the team is hardening its security to reduce privileges and plans to undergo a formal penetration test when the forum is brought back online. Since Kodi is a non-profit and relies on volunteers, the company is asking for volunteers from professional pen test companies to offer their time and expertise. Kodi has also reported this breach to the UK Information Commissioner's Office (ICO) as the forum was hosted in the UK and is sharing the exposed email addresses with Have I Been Pwned (HIBP).
Key Social Engineering/OSINT Themes	• Recon - An inactive Kodi employee's credentials were used to access the MyBB admin console to create and steal backups. It is not yet known how the attacker got hold of these credentials.
Picnic's Recommended Remediations **For An Automated Solution,** **Contact Picnic**	• Regularly audit employee access to one of least privilege (including offboarding). • Monitor and neutralize sensitive information disclosure. In this case, look for credentials that may have been exposed on company repositories. • Regularly review any external facing components to understand exposure. Allow those that are trusted, remove those that are not, and ensure MFA is securely configured for all accounts.
Industry	Software
Actor	TBD
Motivations	Financial
Related Hacks	TBD
Breach Notice/Company Notice	https://kodi.tv/article/important-kodi-forum-data-breach/

Other Sources	https://www.bleepingcomputer.com/news/security/kodi-discloses-data-breach-after-forum-database-for-sale-online/ https://www.securityweek.com/400000-users-hit-by-data-breach-at-media-player-maker-kodi/