

Web portal leaves kids' chats with AI toy open to anyone with Gmail account

Earlier this month, Joseph Thacker's neighbor mentioned to him that she'd preordered a couple of stuffed dinosaur toys for her children. She'd chosen the toys, called Bondus, because they offered an AI chat feature that lets children talk to the toy like a kind of machine-learning-enabled imaginary friend. But she knew Thacker, a security researcher, had done work on AI risks for kids, and she was curious about his thoughts.

So Thacker looked into it. With just a few minutes of work, he and a web security researcher friend named Joel Margolis made a startling discovery: Bondu's web-based portal, intended to allow parents to check on their children's conversations and for Bondu's staff to monitor the products' use and performance, also let anyone with a Gmail account access transcripts of virtually every conversation Bondu's child users have ever had with the toy.

Without carrying out any actual hacking, simply by logging in with an arbitrary Google account, the two researchers immediately found themselves looking at children's private conversations, the pet names kids had given their Bondu, the likes and dislikes of the toys' toddler owners, their favorite snacks and dance moves.

In total, Margolis and Thacker discovered that the data Bondu left unprotected—accessible to anyone who logged in to the company's public-facing web console with their Google username—included children's names, birth dates, family member names, “objectives” for the child chosen by a parent, and most

disturbingly, detailed summaries and transcripts of every previous chat between the child and their Bondu, a toy practically designed to elicit intimate one-on-one conversation. Bondu confirmed in conversations with the researchers that more than 50,000 chat transcripts were accessible through the exposed web portal, essentially all conversations the toys had engaged in other than those that had been manually deleted by parents or staff.

<https://arstechnica.com/security/2026/01/web-portal-leaves-kids-chats-with-ai-toy-open-to-anyone-with-gmail-account/>