Security flaw exposed in home security cameras

February 7 2012

Trendnet, a maker of Web-connected home security cameras, has issued an update to fix a vulnerability that allows Internet users to spy on private video feeds.

Trendnet, a maker of Web-connected home security cameras, has issued an update to fix a vulnerability that allows Internet users to spy on private video feeds.

The security hole, which was revealed nearly a month ago by a blog called Console Cowboys, allows for real-time online access to the home surveillance cameras without the need for a password.

Links to the live video feeds have been posted on Internet message boards such as 4chan and Reddit in recent weeks.

Trendnet addressed the problem in a statement on Monday.

"Trendnet has recently gained awareness of an IP camera vulnerability common to many Trendnet SecurView cameras," the Torrance, California-based firm said.

"It is Trendnet's understanding that video from select Trendnet IP cameras may be accessed online in real time," Trendnet said.

"Upon awareness of the issue, Trendnet initiated immediate actions to correct and publish updated firmware which resolves the vulnerability," it said.

In the statement, Trendnet listed 22 camera models sold since April 2010 which may have the vulnerability and provided a link to a site where camera owners can download a firmware fix.

"Trendnet is aware that this IP Camera security threat may affect your confidence in Trendnet solutions," the company said. "Trendnet extends its deepest apologies to consumers which may be impacted by this issue."