# Security flaw could have let hackers turn on smart ovens

26 October 2017


LG's internet-connected ovens can be remotely set to pre-heat, meaning malicious hackers could create a potential safety risk

A security flaw in LG's smart home devices gave hackers a way to control the household appliances of millions of customers, including the ability to turn on ovens, a computer security firm revealed on Thursday.

Check Point Software Technologies said the vulnerability, called "HomeHack", in the LG SmartThinQ mobile app and cloud application allowed their research team to take over a user's account and control connected appliances such as their oven, refrigerator, dishwasher, washing machine, air conditioner and more.

The HomeHack vulnerability also "gave attackers the potential to spy on users' home activities via the Hom-Bot robot vacuum cleaner video camera," Check Point said in a statement.

LG's internet-connected ovens can be remotely set to pre-heat, meaning malicious hackers could create a potential safety risk.

LG sold 80 million smart home devices across the world in 2016, all of which were potentially affected by the flaw.

But the South Korean electronics giant said it fixed the problem by updating its application in September after being alerted by Check Point.

LG recommends all users update their SmartThinQ mobile phone app as well as each connected home device.

"As more and more smart devices are being used in the home, hackers will shift their focus from targeting individual devices, to hacking the apps that control networks of devices," Check Point head of product vulnerability Oded Vanunu said in a statement.