

?Researchers Find Vulnerability in Smart Home Control Apps?

Submitted by [grigby1](#) on Tue, 09/26/2017 - 1:37pm

Researchers at Rapid7 have discovered that Android applications used to control smart home hubs, Wink Hub 2 and Instead Hub, store sensitive information within configuration files in plaintext form. This sensitive information includes access credentials, which could easily be extracted by attackers if developers do not utilize encryption methods to secure such information in storage. This article further discusses vulnerabilities found within these smart home control Android applications, the security of smart home devices, and ways in which users can reduce the risk of credential theft from mobile applications.

[Motherboard reports "Researchers Find Vulnerability in Smart Home Control Apps"](#)
