CVE-2015-4400 : Backdoorbot, Network Configuration Leak on a Connected Doorbell

fortinet.com/blog/threat-research/cve-2015-4400-backdoorbot-network-configuration-leak-on-a-connected-doorbell

January 22, 2016

FortiGuard Labs Threat Research

By Ruchna Nigam | January 22, 2016

Summary

In March 2015, a Network Configuration Leak vulnerability was disclosed to Ring as part of FortiGuard's Responsible Disclosure process.

The vulnerability existed on their first internet-connected doorbell, Doorbot v1.0 but other posts on the subject show that the vulnerability was ported on newer versions of the connected doorbell as well.

The vulnerability had been granted CVE-2015-4400: DoorBot Network Configuration Leak.
We have issued an Advisory and IPS signatures (**DoorBot.Network.Configuration.Leak**) for the same.
We have not been informed by Ring about any patches issued for the reported vulnerability.

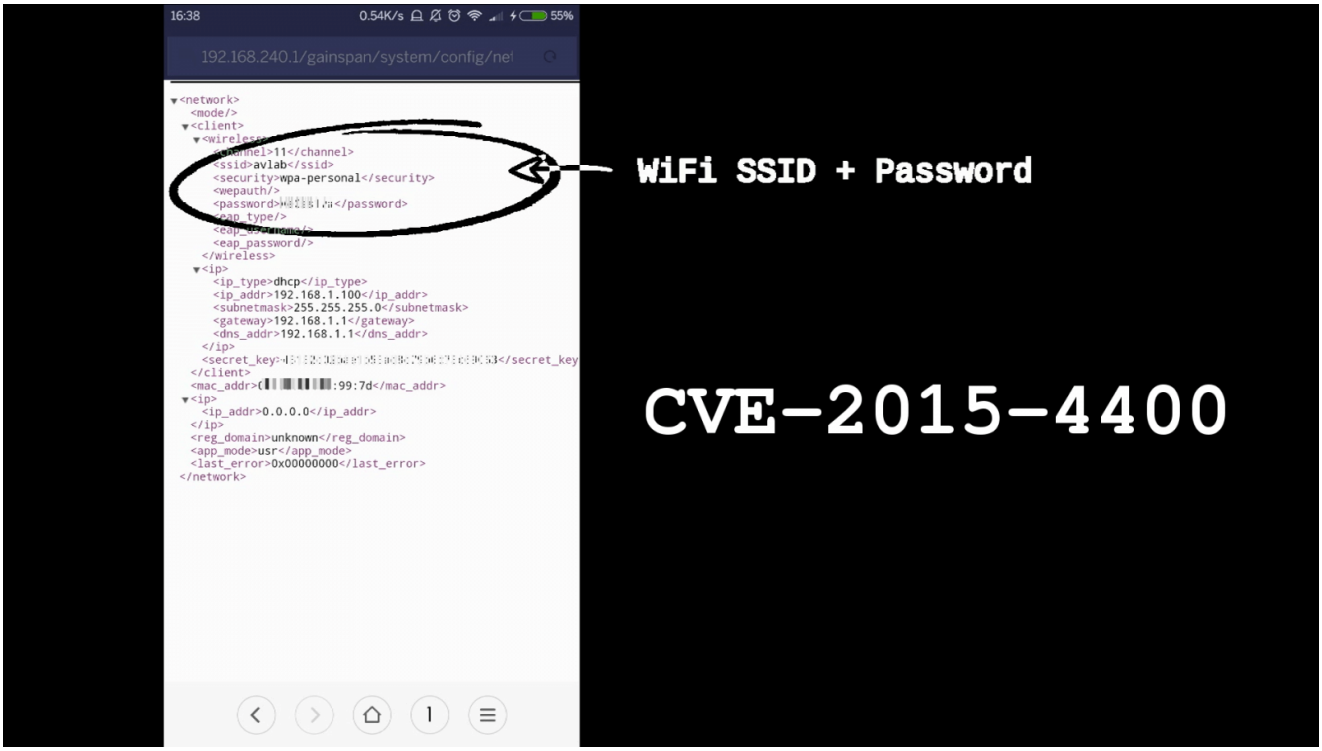
Connected Doorbell?

The Ring, formerly known as Doorbot, is a connected doorbell that comes with network capabilities. It connects to a user's home Wi-Fi and allows the owner to interact with visitors via the doorbell from a smartphone, or receive mobile alerts about every ring on the doorbell. It can also be connected to existing doorbell wiring to allow answering the door using a smartphone.

In March 2015, I found a vulnerability that allows it to let visitors into your home Wi-Fi network as well.

Proof of Concept

Put simply, the vulnerability can be attributed to the poor configuration of it's GainSpan Wi-Fi module that provides an API to recover the Doorbot's network configuration in Plain Text.



On a sidenote, speaking of Plain Text Credentials, the Doorbot Android application analysed in March 2015, stored the logged in users' credentials in Plain-Text on the phone. The good news is this was fixed by Ring soon after in future updates of the application.

Exploitation

Doorbot's claim to security until now was the inaccessibility of the Reset button at the back of the device, thanks to their proprietary screw (that also incidentally is what protects the device from theft).

In my experience with the device, any average Joe screw-driver can be used to unscrew the device and access the Reset button, which ironically has been made more accessible on newer versions of the device.

(Ring image courtesy PenTest Partners)

I guess that leaves us with 'Encryption to the Rescue!' to at least protect your Wi-Fi Credentials.

Not only can the vulnerability be exploited by an attacker when the device is in use, by gaining access to the Reset button, it could also be exploited in the case of Doorbots that are re-sold or discarded, revealing network information from the previous owner/setup at the press of a button.
(We won't be selling our Doorbot anytime soon ;))

More on GainSpan modules

GainSpan Wi-Fi modules are generally used add the 'Internet' to 'Internet of Things' devices i.e. they provide these devices with their ability to connect to the Internet.

They are designed to support two modes of operation :

- **Limited Access Point (AP)** : As the name suggests, while in this mode, the IoT device can act as an Access Point for a limited period of time. In the case of the Doorbot/Ring, this mode is used while setting up the device. When in this mode, the user can connect to the Doorbot's Access Point and, using the Doorbot/Ring mobile application, send it details of which Wi-Fi network it should use. The Doorbot's Access Point is named by the convention DoorbotAp_XXXXXX where the last 6 characters correspond to the end of the Doorbot's MAC Address.
  The device can be made to switch to Limited AP mode by pressing the Reset button illustrated above.
- **Infrastructure Client** : In this mode, the IoT device behaves like any other Wi-Fi capable client and connects to a Wi-Fi network. The GainSpan module, and hence the device it's on, operates in this mode for regular usage.

This is not the first time a poorly configured GainSpan module has leaked a user's network configuration - previously observed on Twine and Wi-Fi Smart Scales stressing the importance of secure configuration and implementation of these ready-to-use technologies on IoT devices.

Although this vulnerability has made *BackDoorbot*a reality, considering the fact that one would need to be within the Wi-Fi network's range to be able to exploit it, a *Doorbotnet*remains a theoretical concept.