

# How Safe Is Your Smart Home?



## Commissioned by

**Ariel Hochstadt**

vpnMentor

Co-Founder

[ariel@vpnmentor.com](mailto:ariel@vpnmentor.com)



## Conducted by

**Alex Costanzo**

Kaizen

[alex.costanzo@kaizen.co.uk](mailto:alex.costanzo@kaizen.co.uk)

**Gancho Ivanov**

InForce Cyber

[office@inforcecyber.com](mailto:office@inforcecyber.com)

# Table of Contents

---

About the Team	<b>3</b>
vpnMentor	3
The Ethical Hacking Team - InForce Cyber	3
Overview	<b>4</b>
Personal Assistant Device - Amazon Echo 1st Generation	<b>5 - 6</b>
1. Smart Lock A - August 1st Generation	<b>7 - 10</b>
1.1. Password Attack	8
1.2. Owner-Level Access Not Revoked	9
2. Smart Lock B - Kwikset Kevo 1st Generation	<b>11 - 12</b>
Smart Doorbell - Ring 1st Generation	<b>13 - 14</b>
Smart Plug - TP-Link HS110	<b>15 - 16</b>
Smart Camera - Samsung SNH-1011	<b>17 - 18</b>
Conclusion	<b>19</b>

---

# About the Team



---




Ariel Hochstadt, former Google Marketing Manager and Head of Research at vpnMentor, commissioned the research.

Internet security experts, vpnMentor, are committed to providing helpful, honest guides on Internet security topics, which can be hard to understand. vpnMentor are dedicated to staying at the forefront of the latest changes in security and ensuring users know how to protect themselves. In the past three months the research team at vpnMentor discovered and published 3 vulnerabilities reports on both Internet devices and software, which were issued 6 prestigious CVE's by The National Cybersecurity FFRDC.

## The Ethical Hacking Team - InForce Cyber

---

InForce Cyber is a security firm that specialise in security assessment, including penetration testing and ethical hacking. The InForce Cyber team comprised of:

-  **Asen Kehayov**; the CEO of InForce Cyber and Ethical Hacker. Asen took the lead on this project and developed a report on the vulnerabilities of the smart home devices tested. Asen is a professional pen-tester and ethical hacker who has a master's degree in cyber security. [Asen can be viewed on LinkedIn here.](#)
-  **Yussef Dajdaj**; an Offensive Security Certified Professional. Yussef is also a professional ethical hacker; he is particularly talented at exploiting vulnerabilities and solving complex problems. [Yussef can be viewed on LinkedIn here.](#)
-  **Gancho Ivanov**; Client relations and project manager. Although the hackers took the lead on researching and testing Gancho was the lead contact, assuring all work was conducted smoothly and that information is relayed in a concise manner. [Gancho can be viewed on LinkedIn here.](#)

These qualified professionals were able to exploit vulnerabilities within some of the most popular smart home devices in the world today. The team uncovered these flaws through intense research and testing and provided clear instructions on how we can protect and prevent the exploitation of such items in the future.

## Summary

---

We evaluated the privacy and security of some of the most popular smart home devices available today in order to assess how likely it is that a malicious actor would be able to hack these devices in order to gain access to private information, including, in some cases, audio and visual footage and sensitive information stored online, such as bank details.

We identified vulnerabilities in all devices tested, including critical vulnerabilities in some. For some devices tested it was found that previous vulnerabilities that manufacturers have released updates to fix can still be exploited, particularly in cases where the devices were connected to a private network and therefore not automatically updating. These issues are also particularly prevalent in second-hand devices.

As well as uncovering these vulnerabilities, we have suggested ways that users can protect themselves from becoming a target.

## Introduction

---

As smart technologies in the home become increasingly mainstream, recent research revealed that nearly a quarter of UK homes now contain at least one smart home device. However, worryingly, although 56% of those who own these devices purchased them for security reasons, 55% admitted that they are not sure how these devices work. With this being the case, smart home technology opens itself up as a lucrative opportunity for malicious hackers to exploit and gain access to your home.

With this opportunity posing a potential public threat, Internet security experts vpnMentor have investigated the potential threat of a number of the most popular smart home devices, including personal assistant devices, smart locks, smart cameras and smart plugs. Utilising an expert team of ethical hackers, we have uncovered the vulnerabilities within each device, as well as the tactics you can employ to protect yourself from becoming a victim of cyber attack within your own home.



# Personal Assistant Device

Amazon Echo 1st Generation

## ✓ Device Safety



Product	Amazon Echo 1st Generation
Camera	No
Microphone	Yes
Connectivity	Bluetooth / Wi-Fi
Material	Metal

## 👁 Overview

Our hacking team tested a popular personal assistant device known for its intuitive design and complex functionality. The 24/7 listening device provides users with the ability to control their smart gadgets with a simple verbal command, making everyday tasks simpler.

## 🏰 Tactics

Taking into consideration the non-stop listening feature, the engagement team focused their efforts on gaining full control over the device. [Further research revealed a critical vulnerability related to the hardware design of the product.](#) The sensitive debugging pads are easily accessible through the base of the device and configuration settings allow the personal assistant to boot from an external source.



# Personal Assistant Device

Amazon Echo 1st Generation



## Exploitation

---

Starting the device from a specially crafted SD card allowed our team to gain administrative control over the underlying operating system and install malicious software, without leaving physical evidence of tampering. Once installed, this malware could grant an attacker persistent remote access to the device, the ability to steal customer authentication tokens and the power to stream live microphone audio to remote services without altering the functionality of the device.

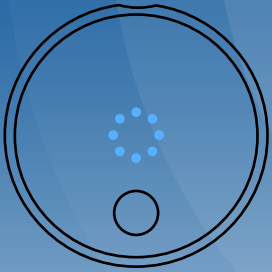


## Recommendations

---

Users can follow a set of simple rules in order to ensure security best practices have been met:

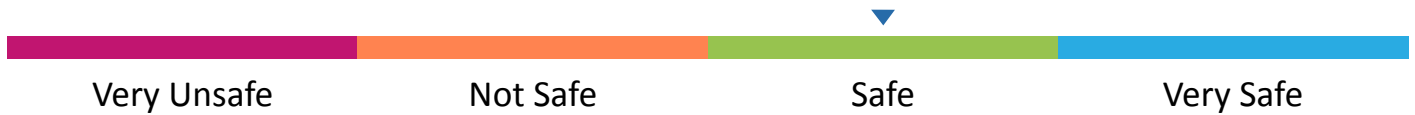
- ✓ Always perform open source research through reliable search engines (e.g. Google, Bing, etc.) on possible vulnerabilities identified for the smart device in which you are interested.
- ✓ Buy your smart gadget from an officially certified source.
- ✓ Be aware of any signs of physical intervention with the product.
- ✓ Stay up-to-date with the latest news around your device.
- ✓ Directly address the seller if you or someone else has identified any major misconfiguration.








# 1. Smart Lock A

August 1st Generation

## Device Safety



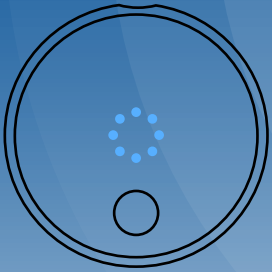
 Product	August 1st Generation Smart Lock
 Camera	No
 Microphone	No
 Connectivity	Wi-Fi
 Material	Aluminum

## Overview

We conducted a comprehensive security assessment on a popular smart-locking device. The innovative Bluetooth door lock attaches to a deadbolt and offers convenience and functionality to its customers. The wireless product relies on various access control mechanisms based on predefined user privileges. Once installed, users can unlock their front door using their smartphone, and grant OWNER or GUEST access to others.

## Tactics

The smart lock classifies users into the two types: OWNER and GUEST. An OWNER user is assumed to be a resident of the house and is effectively an administrator of the system. OWNER level access implies a very high degree of trust, and would typically be granted only to a spouse or a co-owner of the property. A GUEST user is assumed to be someone the OWNER wants to grant temporary house access to.



# 1. Smart Lock A

August 1st Generation

Any user who is not a resident of the house or someone a resident wants to grant access to falls outside of these two groups and should not have any of the permissions of the OWNER or the GUEST.

## Exploitation

---

### 1.1. Password Attack

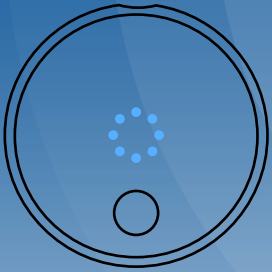
August requires users to go through a simple password verification process when accessing the mobile application for the first time. [The password complexity policy requires the use of at least eight characters, one uppercase letter, one lowercase letter, one numeric symbol, and one special character.](#) After a successful login, the active user session never expires automatically, which is considered a bad security practice. This can potentially pose a risk if an attacker has physical access to the victim's device.

[The mobile application does not require old password verification prior to a password change, which is considered a poor practice from a security standpoint.](#) In this case, our ethical hacking team was able to change the current user password.

However, this attack failed when we tried to log in as the user on another device because the application requires email/SMS verification of the new host machine. [A single-use code is sent to the real user's phone or email account, so a malicious actor without access to at least one of these will not be able to login.](#)

The email/SMS message, however, only includes the verification code with no other information. The message does not suggest to the user than an attacker may be attempting to access their account. This is a low risk vulnerability and is not considered to be a direct threat to the users.





# 1. Smart Lock A

August 1st Generation

## 1.2. Owner-Level Access Not Revoked

Through our investigation, we discovered that owners could still communicate with the lock while offline. This poses a threat in a scenario such as the following:

1. Anna gives Mike OWNER-level access.
2. Anna gets out of Bluetooth range of the smart lock.
3. Mike maliciously puts his phone in airplane mode, preventing it from communicating with the smart lock servers, but leaving Bluetooth enabled.
4. Anna revokes Mike's access.

In this case, Anna is unable to communicate with the lock because she is out of Bluetooth range. She is also unable to communicate with Mike's phone because he has disabled Internet connectivity. Therefore, neither the smart device nor Mike's mobile application will receive the revoking message. Mike can then continue locking and unlocking the door as though his access had not been discontinued. Mike's access cannot be revoked until Anna communicates with the lock.

Furthermore, it seems that there is a bug in the lock's logging code and the log files will not properly report Mike's access during this period. This means that if Mike did access the house in this time while he is offline, Anna would have no way of knowing that he has entered. The above listed issue can be considered as a low risk level vulnerability and it is not considered a direct threat to users.



# 1. Smart Lock A

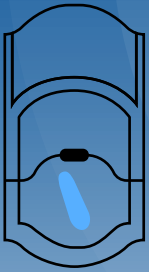
August 1st Generation

## ☆ Recommendations

---

Users can follow a set of simple rules in order to ensure security best practices have been met:

- ✓ Set a complex lock code (passcode, password, passphrase, etc.) for all your personal electronic devices.
- ✓ Do not leave your personal electronic devices unattended in public places.
- ✓ Avoid assigning OWNER privileges to multiple users and follow the principle of “least privilege” - giving a user account only those privileges, which are essential to perform its intended function.
- ✓ Make sure your smart lock access list is up-to-date before you leave home.
- ✓ Avoid using “smart only” locking devices to prevent unauthorized remote control over your protected assets.
- ✓ Always perform an open source research through reliable search engines (e.g. Google, Bing, etc.) on possible vulnerabilities identified for the smart device you are interested in.
- ✓ Buy your smart gadget from an officially certified source.
- ✓ Be aware of any signs for physical intervention with the product.
- ✓ Stay up-to-date with the latest news around your device.
- ✓ Directly address the seller if you or someone else has identified any major misconfiguration.








## 2. Smart Lock B

Kwikset Kevo 1st Generation

### Device Safety



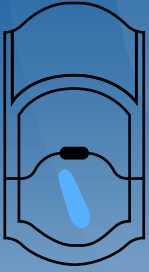
 Product	Kwikset Kevo 1st Generation Touch-to-Open Smart Lock
 Camera	No
 Microphone	No
 Connectivity	Bluetooth
 Material	Metal

### Overview

Our hacking team also conducted an in-depth assessment on a second popular Bluetooth deadbolt device. [This lock actively communicates with all assigned key fobs and mobile devices. Using intelligent positioning technology the smart gadget identifies whether the user is outside or inside the protected area and triggers the unlocking mechanism upon successful verification.](#)

### Tactics

A comprehensive examination of software and hardware configuration revealed possible physical exploitation of the locking mechanism utilising commonly owned tools.



## 2. Smart Lock B

Kwikset Kevo 1st Generation

### Exploitation

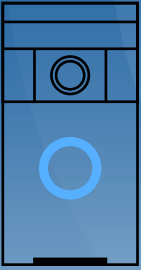
---

By inserting the thin sharp part of a screwdriver into the lock and using a small hammer with precise shaking movements, a malicious actor can reach the alignment point of all pins relatively simply. Further application of rotational pressure using pliers leads to a potential unauthorised access and exposure of valuable assets.

### Recommendations

---

- ✓ Always perform an open source research through reliable search engines (e.g. Google, Bing, etc.) on specific functionality requirements and critical vulnerabilities related to the smart device you are interested in.
- ✓ Be aware of any signs for physical intervention with the product.
- ✓ Stay up-to-date with the latest news around your preferred smart device brand. Directly address the appropriate authorities if you or someone else has identified any major misconfiguration.



# Smart Doorbell

Ring 1st Generation

## ✓ Device Safety



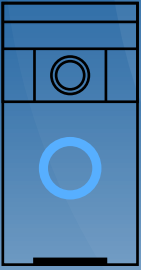
Product	Ring 1st Generation Smart Doorbell
Camera	Yes
Microphone	Yes
Connectivity	Wi-Fi
Material	Hard Plastic

## 👁 Overview

Today's fast growing demand for remotely controllable household devices, and the desire to have eyes on your house at all times, has led to the automation of usually unsophisticated devices, such as doorbells. However, are smart doorbells opening you up to more problems than they're preventing? The target gadget we tested is one of the most popular brands on the global market at the moment, the Ring Smart Doorbell.

## 🏰 Tactics

Following device logic, our ethical hacking team's main goal was focused on obtaining administrative privileges and gaining access to the camera feed for surveillance purposes. However, the question remained whether this was truly the highest level of access they could gain from an IoT (Internet of Things) device connected directly to the home wireless (Wi-Fi) network.



# Smart Doorbell

Ring 1st Generation

## Exploitation

---

In order to control a smart doorbell device, users have to connect it to an externally accessible wireless network. Once connected, the device can be managed through a convenient mobile application.

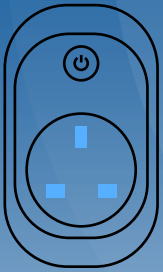
During investigations, the team noticed an orange button on the back of the doorbell device that can be easily accessed by a malicious actor using a regular screwdriver. [Once the button is continuously pressed, the hardware device turns into an unprotected Wi-Fi access point \(AP\).](#)

Connecting to the Ring AP gives a malicious actor the opportunity to enumerate device internal configuration details. [The hacking team then discovered an interesting web address which reveals the password of user's home Wi-Fi network thus providing external attackers access to sensitive personal information which can then be further leveraged to give an attacker full control over the victim's private network.](#) Once this access is gained, attackers can access sensitive personal information stored by users of the Wi-Fi network online, for example online banking details.

## Recommendations

---

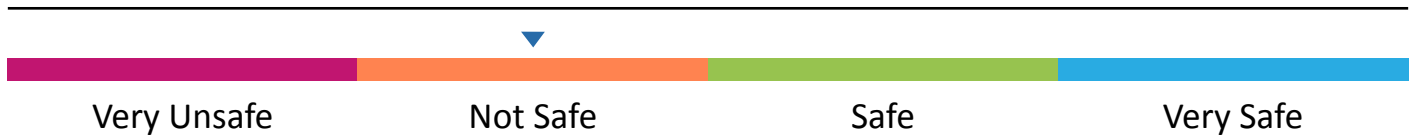
- ✓ Keep your externally facing smart devices on a separate network.
- ✓ Always perform an open source research through reliable search engines (e.g. Google, Bing, etc.) on possible vulnerabilities identified for the smart device you are interested in.
- ✓ Be aware of any signs for physical intervention with the product, even once installed.
- ✓ Make sure your smart device is properly configured and regularly updated.








## Smart Plug

TP-Link HS110

### Device Safety



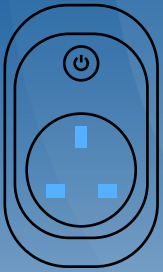
 Product	TP-Link HS110 - Smart Plugs With Energy Monitoring
 Camera	No
 Microphone	No
 Connectivity	Wi-Fi
 Material	Hard Plastic

### Overview

As more and more of the public become interested in living in a connected home, smart plugs offer a simple way to make your existing appliances smarter. Using these plugs allows you to control any electronic appliance from the ease of your smartphone. [The industry leaders of these plugs provide customers with power management, remote on/off switching, intelligent timer, and task scheduling.](#)

### Tactics

The ethical hacking team executed comprehensive intelligence gathering and vulnerability enumeration procedures for the popular smart plug device. The primary goal was to understand the product's functional logic and trick the device to execute our commands. If successful, this attack would provide malicious actors with the ability to control high criticality appliances and potentially cause serious material damage.



## Smart Plug

TP-Link HS110

### Exploitation

---

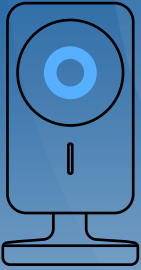
By using dedicated testing tools, the team successfully communicated with the target device and found a lack of properly implemented encryption and authentication security mechanisms. The team managed to send valid on/off commands, which were scheduled to execute after a specific period of time. A detailed analysis confirmed the ability of random users, connected to the same network, to take full control over the device from the devices' owners and cause denial of service to other in-range smart appliances.

### Recommendations

---

- ✓ Always perform an open source research through reliable search engines (e.g. Google, Bing, etc.) on possible vulnerabilities identified for the smart device you are interested in.
- ✓ Keep your externally facing smart devices on a separate network.
- ✓ Be aware of any signs for physical intervention with the product.
- ✓ Make sure your smart device is properly configured and regularly updated.
- ✓ Unplug any devices that could potentially cause physical damage to your home if left on (for example, heat styling tools) from their smart plugs when not in use.





# Smart Camera

Samsung SNH-1011

## ✓ Device Safety



Product	Samsung SNH-1011 - Smart Camera
Camera	Yes
Microphone	No
Connectivity	Wi-Fi
Material	Aluminum

## 👁 Overview

The ability to monitor and control our homes and businesses remotely has been the main focus of various technology companies over recent years. Smart cameras, accessible through the Internet, bring significant convenience for users worldwide and peace of mind to parents and pet owners concerned about loved ones at home while they are away. People have the ability to monitor, zoom in and out, move, change vision mode, record, and much more just by using a simple mobile application.

## 🏰 Tactics

The testing approach in this case was mainly directed to obtaining access to the camera feed and potentially escalating the privilege level to administrator. After completing a complex in-depth analysis of the application source code, the team noticed poor validation practices related to the password reset process. [This misconfiguration provided a reliable attack vector, which could be further escalated by the ethical hackers.](#)



## Smart Camera

Samsung SNH-1011

### Exploitation

---

By utilising manual testing techniques, we were able to establish the smart camera IP address and exploit a vulnerability which allows an attacker to successfully complete a password reset for the administrative account without knowing the original password.

This critical issue occurs because of a poorly coded script used for initial administrative account set up. The misconfiguration allows an attacker to call the same script after the original password has already been created. By exploiting this weakness, the team was able to reset the pre-existing administrative password and gain full control over the wireless camera with relative ease.

This vulnerability means that a malicious actor could gain full access to the very camera footage from inside your home that you set up to protect it. This is particularly concerning when considering the fact that the product is largely marketed towards, and used by, parents watching over their young children.

### Recommendations

---

- ✓ Always perform an open source research through reliable search engines (e.g. Google, Bing, etc.) on possible vulnerabilities identified for the smart device you are interested in.
- ✓ Keep your externally facing smart devices on a separate network.
- ✓ Be aware of any signs for physical intervention with the product.
- ✓ Make sure your smart device is properly configured and regularly updated.

# Conclusion

In the modern world, you don't need to fear the growth of technology and the ever-expanding wealth of smart devices at our fingertips. However, [if you are going to introduce smart technology into your home, it is important that you remain vigilant with your devices to ensure that only those you trust have access.](#)

Following a set of simple rules in order to ensure security best practices have been met will save you from becoming an easy target for cyber, and in some cases physical, crime. Below are the key factors to remember:

- ✓ Set a complex lock code (passcode, password, passphrase, etc.) for all your personal electronic devices.
- ✓ Do not leave your personal electronic devices unattended in public places.
- ✓ Avoid assigning administrative privileges to multiple users and follow the principle of "least privilege" - giving a user account only those privileges, which are essential to perform its intended function.
- ✓ Make sure your smart device is properly configured and regularly updated.
- ✓ Always perform an open source research through reliable search engines (e.g. Google, Bing, etc.) on specific functionality requirements and critical vulnerabilities related to the smart device you are interested in.
- ✓ Only ever buy your smart devices from officially certified sources.
- ✓ Keep your externally facing smart devices on a separate network.
- ✓ Be aware of any signs for unauthorized physical intervention with your device.
- ✓ Stay up-to-date with the latest news around your preferred smart device brand.
- ✓ Directly address the appropriate authorities if you or someone else has identified any major misconfiguration with any of your smart home devices.