

Bitdefender[®]

Ring Video Doorbell Pro Under the Scope

Internet-connected doorbells with motion-sensing and notification capabilities have become extremely popular among smart-home enthusiasts. So popular, in fact, that vendors such as Amazon have enrolled their devices in “neighborhood watch” programs aimed at curbing cyber-crime by [granting law enforcement access](#) to security footage.

As the creator of the world’s first smart-home cybersecurity hub, Bitdefender constantly audits popular pieces of IoT hardware for vulnerabilities that might affect customers if left unaddressed. Any issues identified are fed into the Bitdefender BOX Vulnerability Assessment technology and are privately reported to affected vendors, as per our responsible vulnerability-disclosure policy.

Bitdefender researchers have discovered an issue in Amazon’s Ring Video Doorbell Pro IoT device that allows an attacker physically near the device to intercept the owner’s Wi-Fi network credentials and possibly mount a larger attack against the household network. This vulnerability was communicated to the vendor privately as per the timeline below.

At the moment of publishing this paper, all Ring Doorbell Pro cameras have received a security update that fixes the issue described herein. We appreciate the Ring team’s efforts to mitigate the issue and keep their customers safe

Disclosure timeline

Jun 20, 2019: Bitdefender makes first contact with Amazon and requests a secure communications channel for disclosure

Jun 24, 2019: Vendor sends back requested PGP key; Bitdefender sends vulnerability details over secure channel

Jul 16, 2019: Bitdefender is invited to send the report via the HackerOne bug bounty program

Jul 18, 2019: HackerOne report is acknowledged and accepted

Jul 30, 2019: Bitdefender requests an update from the vendor

Aug 16, 2019: Vendor closes the report and marks it as a duplicate without saying whether a third party already reported this issue

Sep 05, 2019: After some back and forth with the vendor, a fix is being partially deployed

Nov 7, 2019: Coordinated responsible disclosure



Vulnerability summary

Cloud-device communication

The Ring Video Doorbell only communicates via the company's cloud services using multiple API endpoints, such as **es.ring.com** or **ps.ring.com**. To communicate with these endpoints, it uses HTTPS while verifying the server certificates, making a man-in-the-middle attack impossible.

To quickly handle any events, the device always keeps a connection open to the cloud. This speeds up the response because, instead of waiting for a poll from the device, the server can send the information as soon as it is needed.

Local network

The device uses the local (residential wi-fi) wireless network to connect to the Internet, but it exposes no services to the local network. All communication takes place through the vendor's cloud services. This dramatically decreases the local attack surface, but halts service when the internet connection is down (the ring feature still works, so the user can hear that somebody is at the door).

Device initial configuration

- **Information leak [1]**

The device uses a wireless connection to join the local network. When first configuring the device, the smartphone app must send the wireless network credentials. This takes place in an unsecure manner, through an unprotected access point. When entering configuration mode, the device creates an access point without a password (the SSID contains the last three bytes from the MAC address).

Once this network is up, the app connects to it automatically, queries the device, then sends the credentials to the local network. All these exchanges are performed through plain HTTP. This means the credentials are exposed to any nearby eavesdroppers.



Smartphone app – cloud communication

- **Account management**

Each user is required to register a Ring account. The device is linked to the user account.

To communicate with the device, the smartphone application always uses the cloud services, even when on the same local network. The functionality is handled by the **api.ring.com** API endpoint. The app also communicates with other APIs for other functionalities, such as error reporting, notifications, etc. All these connections are made securely over TLS while performing certificate pinning.

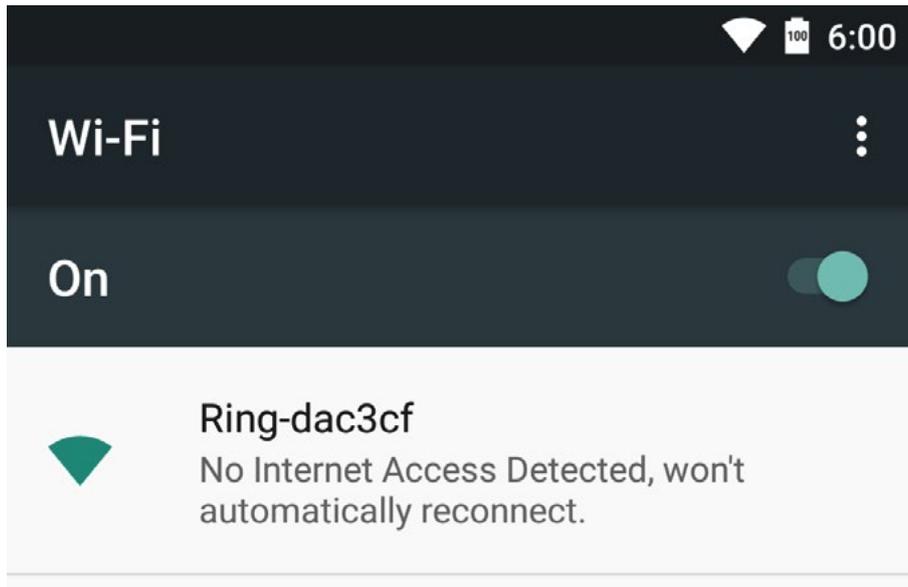
- **Device access control**

Only the legitimate owner can access and control the doorbell. Functionality exists for others to access the device and the user can give this permission through the app.

Access to the devices is thoroughly enforced so nobody can access a doorbell without the required permissions.

[1] Credentials leak detailed

As shown above, the credentials of the local wireless network are sent through an unsecure channel (an open network). This can be exploited by a nearby attacker to obtain the user’s network credentials.



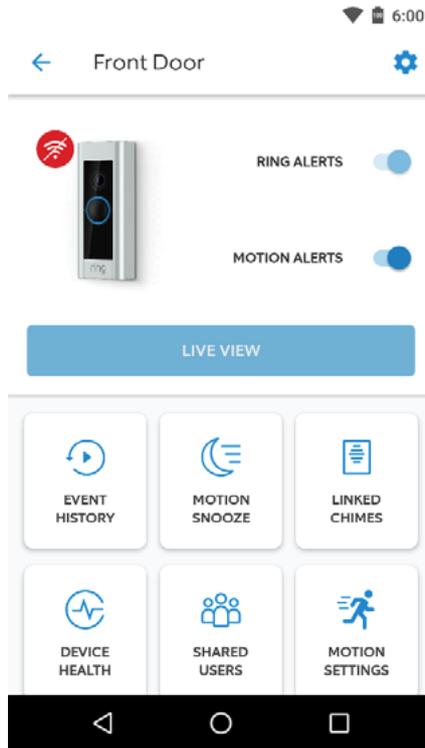
The attacker must trick the user into believing that the device is malfunctioning so the user reconfigures it. One way to do this is to continuously send deauthentication messages, so that the device is dropped from the wireless network.

```
11:31:38 Sending 64 directed DeAuth (code 7). STMAC: [E0:4F:43: [REDACTED]] [ 0|73 ACKs]
11:31:38 Sending 64 directed DeAuth (code 7). STMAC: [E0:4F:43: [REDACTED]] [ 0|76 ACKs]
11:31:39 Sending 64 directed DeAuth (code 7). STMAC: [E0:4F:43: [REDACTED]] [ 0|62 ACKs]
11:31:40 Sending 64 directed DeAuth (code 7). STMAC: [E0:4F:43: [REDACTED]] [ 0|61 ACKs]
11:31:40 Sending 64 directed DeAuth (code 7). STMAC: [E0:4F:43: [REDACTED]] [ 0|61 ACKs]
11:31:41 Sending 64 directed DeAuth (code 7). STMAC: [E0:4F:43: [REDACTED]] [ 0|59 ACKs]
11:31:41 Sending 64 directed DeAuth (code 7). STMAC: [E0:4F:43: [REDACTED]] [ 2|64 ACKs]
11:31:42 Sending 64 directed DeAuth (code 7). STMAC: [E0:4F:43: [REDACTED]] [ 1|67 ACKs]
11:31:43 Sending 64 directed DeAuth (code 7). STMAC: [E0:4F:43: [REDACTED]] [ 0|70 ACKs]
11:31:43 Sending 64 directed DeAuth (code 7). STMAC: [E0:4F:43: [REDACTED]] [ 0|39 ACKs]
11:31:44 Sending 64 directed DeAuth (code 7). STMAC: [E0:4F:43: [REDACTED]] [ 0|54 ACKs]
11:31:44 Sending 64 directed DeAuth (code 7). STMAC: [E0:4F:43: [REDACTED]] [63|96 ACKs]
11:31:45 Sending 64 directed DeAuth (code 7). STMAC: [E0:4F:43: [REDACTED]] [ 0|58 ACKs]
11:31:46 Sending 64 directed DeAuth (code 7). STMAC: [E0:4F:43: [REDACTED]] [ 0|67 ACKs]
```

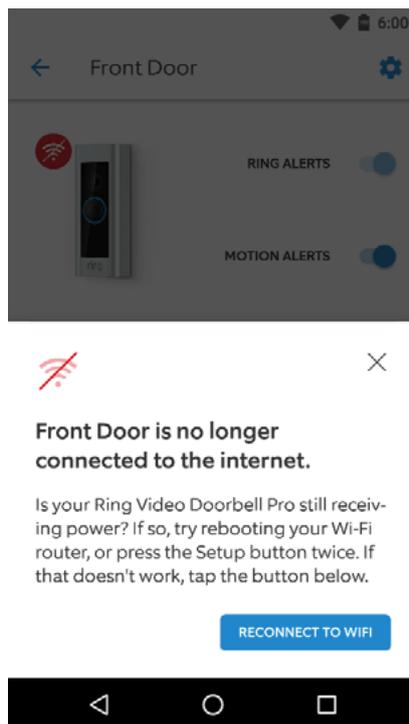
[4]



Deauthentication is the process that allows a third party to mount the attack. It must be performed until the owner notices that the device misbehaves. This might take a while, because the doorbell will still ring the chime when the button is pressed. The only difference is that it will not send a notification and cannot be reached by the remote servers. After a while, the app will show the device as offline:

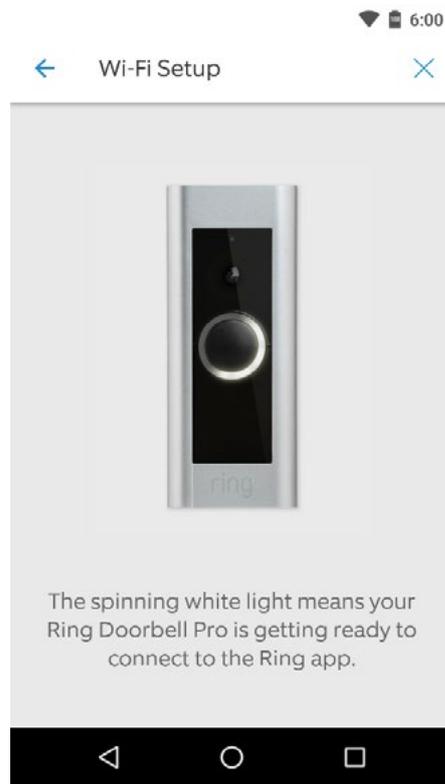
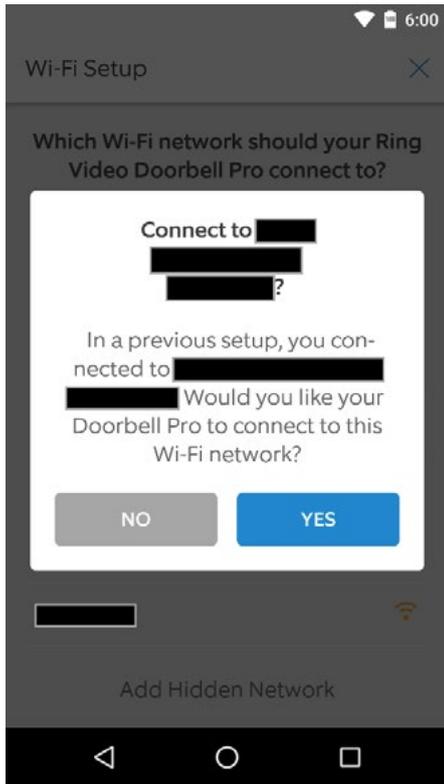


The “live view” button becomes greyed out and, when clicked, the app will suggest restarting the router or pressing the setup button twice on the doorbell. Pressing the button twice will trigger the device to try to reconnect to the network – an action that will fail. The last resort is to try and reconfigure the device.





Reconfiguring the device:



Meanwhile the attacker is sniffing all the packets, waiting for the plaintext credentials to be sent to the device.

```
Host: 192.168.240.1
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 499
```

```
<network>
  <client>
    [REDACTED]
    <wireless>
      <ssid>myhomenetwork</ssid>
      <channel>1</channel>
      <security>wpa-personal</security>
      <password>pwnedpassword</password>
    </wireless>
    <ip>
      <ip_type>dhcp</ip_type>
    </ip>
  </client>
```

```
</network>HTTP/1.0 200 OK
Content-Type: text/xml
Content-Length: 19
```

```
<status>ok</status>
```



This page is left blank intentionally



Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers.

More information is available at <http://www.bitdefender.com/>.

All Rights Reserved. © 2019 Bitdefender. All trademarks, trade names, and products referenced herein are property of their respective owners. FOR MORE INFORMATION VISIT: enterprise.bitdefender.com.

