## 1.How/where was it released?

The Ring Hacks started in 2019 but was a series of incidents that is still has pending legal matters. The exact release date of the initial exploit is unknown, but the first reports of the vulnerabilities suspected in the Ring security camera hacks began in June of 2019 when Bitdefender first made contact with Amazon to disclose the vulnerability they discovered in the Ring Video Doorbell cameras.(Bitdefender: [Source](https://www.bitdefender.com/files/News/CaseStudies/study/294/Bitdefender-WhitePaper-RDoor-CREA3949-en-EN-GenericUse.pdf)) The vulnerability could be exploited through the wi-fi between the ring device, when it creates an unprotected wireless access point, and the application on the user's phone when it connects to it in order to pass the wireless network credentials in plain text over an unsecure HTTP connection which would not only allow attackers to eavesdrop this connection to obtain the local wireless credentials but they could also trigger the reconfiguration of the Ring Video Doorbell by “continuously sending reauthentication messages so that the device gets dropped from the wireless network. At this point, the mobile app loses connectivity and instructs the user to reconfigure the device” (ECcouncil: [source](https://cisomag.eccouncil.org/researchers-find-vulnerability-in-amazons-ring-video-doorbells/)) where the attacker could then learn the ring device's configuration settings and application credentials. By September 5th, Ring reported that all the cameras had received a patch to address the issue and by November 7th, the Bitdefender report was published in a white paper to the public.

This does not seem to be the only vulnerability for Ring. Even after the November 7th publication various customers began to report that they had been hearing strange voices over their speakers or noticing that the blue light was lit on the device indicating that someone was ‘watching’ even though no one authorized was accessing the camera; this indicated that a wider hack had occurred.

## 2. How was it detected?

As noted above the vulnerability leading to the hack was first reported in June of 2019 via a responsible disclosure by Bitdefender to Amazon/Ring. Suspected exploits Ring systems were also reported in 2019 when dumps of valid ring credentials ended up online and users reported noticing their camera was active when they were not aware of authorized access.

Ring took the position that they have “no evidence of an unauthorized intrusion or compromise of Ring’s systems or network.” Regardless, it is possible individual customers could have been compromised through credential stuffing using already leaked credentials from other sites. (Consumer Reports: [source](https://www.consumerreports.org/hacking/3000-ring-doorbell-and-camera-accounts-may-be-vulnerable-to-hackers-a3229685651/)) This could also account for how over 3,672 customer accounts were found to have been leaked on a dark web site as early as December 2019. One source, ‘Techcrunch’, claims that an unnamed security researcher reported on Thursday December 19th to Amazon that they discovered “1,562 unique email addresses and passwords associated with Ring doorbell customers”, but was asked not to make those findings public.

Another source, Buzzfeed (Buzzfeed: [source](https://www.buzzfeednews.com/article/carolinehaskins1/data-leak-exposes-personal-data-over-3000-ring-camera-users)), posted an article on December 19th that reported a man called ‘Nick Shepherd’ had contacted Ring’s customer support line with a list of over 3,600 “exposed log-in emails, passwords, time zones, and the names of people to specific Ring cameras”, but was told at the time by Ring they “could not assist him”. Instead, he decided to post the leak to a cybersecurity-related subreddit page on December 16th which was met with a public announcement from Ring on December 18th: “Ring has not had a data breach. Our security team has investigated these incidents and we have no evidence of an unauthorized intrusion or compromise of Ring’s systems or network…It is not uncommon for bad actors to harvest data from other company's data breaches and create lists like this so that other bad actors can attempt to gain access to other services.”

There is also speculation in these articles that the data is too formatted to have been stolen from customers directly and that this data would only be easily available from a company database; and would imply that Ring was compromised. The company, however, “denies any claims that the data was compromised as a part of a breach of Ring’s systems.” Ring later addressed a notice to those impacted by the breach informing them of steps to take to protect themselves.

## 3. What damage was inflicted?

Damage to Ring customers was primarily emotional and breach of expected privacy, which is difficult to quantify, especially since many users may not even know if they were victims. In some cases, people were subject only to verbal threats and racist comments made over their speakers. In other cases, however, the damage to victims was significantly more invasive. One couple shared a video of their bedroom, at which point a voice command over their speaker and claims that he can see them. ([source](https://abcnews.go.com/US/ring-security-camera-hacks-homeowners-subjected-racial-abuse/story?id=67679790)) Another family shared their experience, which involves a camera put up to supervise their young daughters while they were at work and instead it wound up letting a strange man watch, record and interact with minors. ([source](https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html)) Yet another incident occurred wherein an elderly woman living in a facility was sexually harassed through the camera and was allegedly so distraught that she had to move back in with her family because she felt so unsafe. In one final incident, some victims also faced blackmail & ransom attempts from their virtual abusers ([source](https://www.inc.com/minda-zetlin/ring-camera-hacked-hackers-bitcoin-ransom-security.html)).

It goes without saying that the implications of such hacks to the victims are much more serious than the anecdotal evidence might indicate and culminate in serious reputational damages for the company. The hack, its victims, and company responses were covered across news stations and journalistic articles through the end of 2019 and into Q1 2020. The series of negative articles published about the company’s practices and a subsequent lawsuit which negatively impacted the share price of the company. The company’s stock price fell from a high of 25.55 USD in Feb, 21 2020 to 16.80 USD by Mar, 20th 2020. Amazon/Ring also faced a myriad of lawsuits at the federal level and state levels. The most notable of which is a customer class action lawsuit filed in the U.S. district court in the Central District of California based on the claims that "Ring failed to meet this most basic obligation by not ensuring its Wi-Fi-enabled cameras were protected against cyber-attack, notably, Ring only required users enter a basic password and did not offer or did not compel two-factor authentication” and was seeking an upwards of 5 million dollars (ABCnews: [source](https://abcnews.go.com/US/amazon-ring-face-million-proposed-class-action-lawsuit/story?id=67948687)).

## 4.What remediations were put in and by whom?

Ring has continuously denied that their cybersecurity protocols are to blame for the hacks, saying that they are certain that the issue is “in no way related to a breach of compromise of Ring’s security” and has not implemented or reported any company data protection controls related to this leak. Instead, they have cited that people often use similar or identical usernames and passwords for other services and attackers likely used credential stuffing for the various incidents that occurred. Even at the time of the initial vulnerability disclosure Ring already offered optional MFA which would have helped prevent the unauthorized access of their ring accounts. (Consumer Reports: source).

With that said, Ring announced in late 2020 that they have decided to ‘expand’ optional end-to-end encryption offering to some hardwired camera and doorbell devices under their brand, though the option was made available as early as January 2021 it was not an enforced feature. This is not standard encryption in-transit followed by encryption at-rest, but they added an additional envelope around their standard encryption processes with a key managed by the user. In simple terms, they have made it so the video footage can only be viewed by the person in possession of your smartphone and/or tablet connected to it. In more technical terms, “videos are encrypted with keys that are themselves encrypted with an algorithm that creates a public and private key. The public key encrypts, but the private key is required to decrypt.” Only users have access to the private key, which is stored on their smartphone and decrypts the symmetric key, and by extension, encrypted videos. That means that for someone to hack your camera, they would instead have to hack your physical smartphone to access your ring connected devices. This implementation also means that Ring is unable to view any of your footage and cannot turn it over to any kind of law enforcement department.

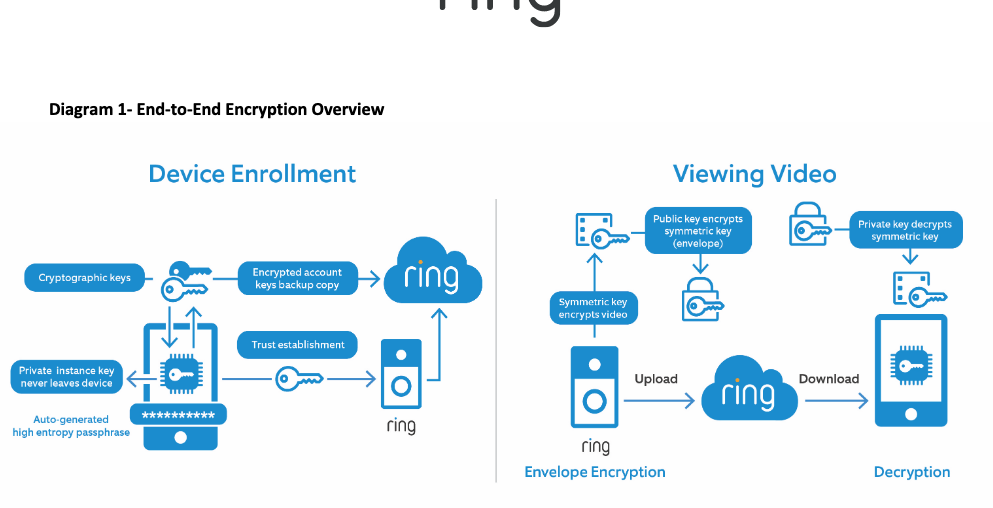
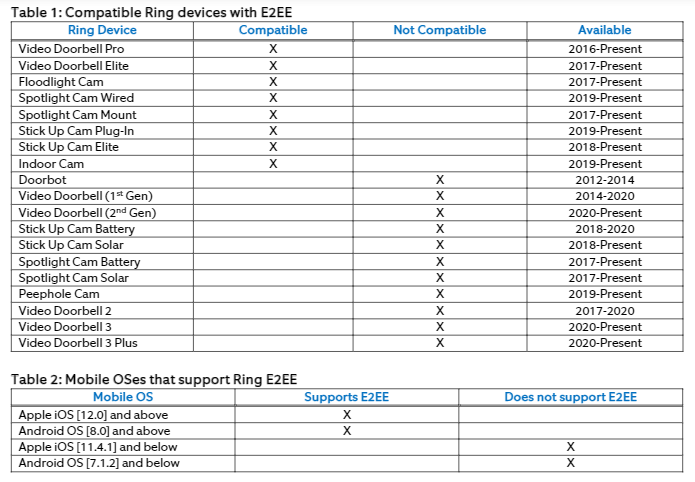


Figure 1‑1 (Source: Ring E2EE Whitepaper)

It is also important to note that amazon does maintain a backup of the keys used for their E2EE process and cloud. (Ring E2EE Whitepaper: [source](https://assets.ctfassets.net/a3peezndovsu/5ihit68yvJLf0IJ2dOHfuO/b9063f50382bbf3e143173bbf49e9781/Ring_Encryption_Whitepaper_2021-07-13.pdf)).

There are limitations to the patch, however, as battery-powered products and earlier generations of the product are still *not* able to have this feature enabled, which means a large population of the popular devices under the Ring brand is excluded from this security see Venturebeat: “Table 1: Compatible Ring devices with E2EE”.



(Venturebeat: [source](https://venturebeat.com/2021/01/13/ring-rolls-out-end-to-end-video-encryption-after-a-class-action-lawsuit/))

In addition, enabling end-to-end encryption disables a host of other features, including voice control through Alexa, the Ring Neighbors network, shared user accounts and remote access to video feeds and recordings. Consumer Reports was able to test the data privacy and security of the new Ring cameras featuring this updated security and have rated their data security ‘very good’, while their data privacy is rated only ‘fair’. (Consumer reports: [source](https://www.consumerreports.org/ring/ring-offers-end-to-end-encryption-for-some-cameras-doorbells-a1063459243/))

## 5.What were the crucial enablers for this disaster in retrospect?

One of the primary crucial enables for these events was the alignment and direction of the products and services at Ring. Ring has expanded their service offerings in many ways that are reliant on access to their customers’ videos, such as their Neighbors App and their Protect Plans. The desire to generate additional reoccurring revenue from these customers led to the commoditization of the data rather than prioritizing the protection of it. As noted above adding the enhanced protections disables several of their other capabilities. Even beyond the internal business needs, The Guardian article shows, Ring had signed contracts with the police that allow the company to send stills or video to law enforcement in over 1,000 cities across the globe. (The Guardian: [source](https://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats)) In addition, over 700 police departments in the US alone had signed contracts that would allow them to acquire footage from private citizens without getting a warrant. The company also handed out free cameras to law enforcement departments who helped them gain new customers in the area which shows the prioritization of company growth and connections over the safety, security, and privacy of their customers.

Ring’s product alignment was also miscalculated with respect to their balance between ease and flexibility for users relative to the security and privacy implications. MFA was offered as an optional setting for users but was not a promoted setting or enabled by default. Logins from unknown IPs or devices were not required to undergo any additional authentication, which may have been an acceptable mitigation rather than enforcing MFA on users who have selected the product for its ease of use.

Third, the confidence in their security capabilities was another enabler for this event. In disaster response the company's message to the community was to place the blame on the ignorance of their customers. It was suggested these accounts may have been compromised by using the same login and password that were exposed in a data leak from a different company. If this was true this suggest a very poor security operations posture given they did not detect any atypical login activity or a spike in attempts.

Fourth, at a technical level the major enabler, according to Bitdefender, was the initial HTTP communication between the device and the mobile app rather than HTTPS. Using HTTPS would have helped protect the WIFI-password in transit and therefore all the traffic on your network.

## 6.What could have been done better by the manufacturers or operators in question?

One thing Ring should have done better is implement more standard authentication practices. As noted in court records from a lawsuit against Ring, “Ring does not require users to implement two-factor authentication. It does not double-check whether someone logging in from an unknown IP address is the legitimate user. It does not offer users a way to view how many users are logged in. It offers no protection from brute-force entries… Even though these basic precautions are common and unexceptional security measures across a wealth of online services, Ring does not utilize them for its service.”(GeekWire: [source](https://www.geekwire.com/2020/ring-customers-cameras-breached-hackers-sue-amazon-proposed-class-action-lawsuit/)) Preventing brute-force attacks and concurrent sessions on the same account are fundamentals and documented in NIST standards such as SP 800-171 and SP 800-53. There are many mitigations that can be put in place that still allow for a good user experience without harming security. With respect to not enforcing MFA, they could have added notifications of new-login activity, or only prompted for another factor of authentication when logging in from an unknown IP or device.

Ring should have improved its security operations posture as they were unable to detect numerous breaches. As noted in the section above, if credentials from other companies’ systems were attempted against Ring’s systems, they should have detected at least some of these attempts. This suggests that there is minimal if any security alerting established on application-level logs. Furthermore, it suggests poor staffing if even after review when incidents had been in the news they were not able to identify any breaches. Ring should ensure proper logging, alerting and staffing as needed to support their business both at the corporate and product levels.

Based on the consumer reports article, which covers the rollout of end-to-end encryption on ring devices in July 2021, this solution should have been made available by the manufacturers to its consumers from the first release of the product. However, the issue remains that the end-to-end encryption requires user opt-in within the device application settings, further described on Ring’s privacy webpage (Ring Privacy page: [source](https://ring.com/privacy)). If implemented, user local Wi-Fi passwords would not have been sent over HTTP where they could be easily intercepted. Additionally, the manufacturers only optionally offered two factor authentication on their devices in 2019. This feature would have helped to prevent a third party with stolen credentials from accessing the device as the additional verification would have at least notified the device owners of the attempted access or have given them some control to stem the attempt as it occurred.

One could also argue that operators of the devices are unaware or uneducated in the security settings available on these devices or used weak/similar passwords used in other services in their lives which made this attack even more possible. However, the company felt it necessary to also send an email to the impacted customers in December of 2019, reporting a data privacy breach and detailing how to activate two-factor authentication and to change their password. Rather than just sending an email they could have made a technical change that required all users to set new passwords on next-login.

## 7. Is this likely to recur and/or how do we prevent this in the future?

The likelihood of this issue recurring is very high. By all accounts, Ring only implemented basic security features prior to and following their class action lawsuit. While the features discussed should have been put in place long before any data was compromised, what truly needs to be examined is the assertion that Ring was not actually the one hacked in 2019 as Ring claimed to have no knowledge of and had denied any kind of company data breach.

Since there is a tremendous onus put on the consumers in this case, one of the most important things that can be done regardless of any updates or patches is to educate the customers. If Ring is not going to make sure their customers know their options regarding security, then they should make the encryption and two-factor authentication a mandatory part of their software instead of leaving it up to every person who buys one of their products. Ring’s contracts with law enforcement agencies also need to be assessed if only because it seems like a gross invasion of privacy for a company to have access to *and permission to pass on* your home, your person, and your family on camera.

In this day and age, a security company should not have to be told that they need to keep their customers' information safe and to keep their users educated however the company has shown in failing this that they need to have a better security posture to not only address complaints of this nature immediately, but also enhance their due diligence processes, security reviews, and privacy assessments in their product offerings as they are currently designing their products with mostly optional security features. Two-factor authentication is a minimum security feature that the company has only recently made mandatory for every customer for their own safety, so end-to-end encryption should be no different and made available on every single device.