Dojo By BullGuard Cybersecurity Experts Identify Major Vulnerability In Amazon's Ring Video Doorbell

Submitted by: The PR Room
Wednesday, 27 February 2019

Unencrypted transmission of audio and/or video footage to the Ring application allows for undetectable arbitrary surveillance and injection of counterfeit traffic, compromising home security and putting family members at risk

BARCELONA MOBILE WORLD CONGRESS and LONDON – FEBRUARY 27, 2019 – Cybersecurity expert, Yossi Atias, General Manager, IoT Security at Dojo by BullGuard (https://dojo.bullguard.com/service-providers/), the market leading IoT security platform for Communication Service Providers (CSPs), took the stage today at Mobile World Congress to demonstrate a live hack of the Amazon Ring video doorbell, exposing a previously unknown vulnerability in the popular IoT device. The hack revealed unencrypted transmission of audio and/or video footage to the Ring application allows for arbitrary surveillance and injection of counterfeit video traffic, effectively compromising home security and putting family members' safety at risk.

Launched in 2012 and acquired in February 2018 by Amazon, the main feature of the Ring video doorbell is two-way communication between the smart video doorbell and the user's mobile app, which acts as a security camera and allows the user to confirm who is ringing their doorbell from anywhere in the world via the internet. Presuming the Ring owner is away from home, they can see who is at their door and then remotely open the door if a supported smart lock is installed to let the housecleaner or babysitter in, for example.

The Ring video doorbell vulnerability lies between the cloud service and the Ring mobile application. In the Ring video doorbell hack, Atias was able to change the video feed so the end user 'believed' they were seeing someone they know and let in previously.

"Ring is a well- respected IoT brand, however, the vulnerability we discovered in the Ring video doorbell reveals even highly secure devices are vulnerable to attack," said Atias. "This particular vulnerability is complex because it is between the cloud and the Ring mobile app, and is acted upon when the Ring video doorbell owner is away from home – meaning the package delivery person, housecleaner or babysitter might not actually be the same person at your door. Letting someone you 'think' you know into your home could potentially have dire consequences, particularly if your kids are at home."

Dojo's cybersecurity experts were able to gain access to the application traffic without difficulty and noted that if the Ring owner is at home, Wi-Fi access – either cracking weak encryption (if present) or exploiting another smart home device is needed. When the owner is in transit, a hacker can open a rogue Wi-Fi connection near the owner and wait for them to join, or join a common public network. Once sharing a network, a simple ARP spoof (https://en.wikipedia.org/wiki/ARP_spoofing) allows the hacker to capture Ring data traffic before passing it on to the mobile app, and certain 3G/4G configurations may allow intra-network poisoning as well. Encrypting the upstream RTP (Real-Time Transport Protocol (https://en.wikipedia.org/wiki/Real-time_Transport_Protocol)) traffic will not make forgery any harder if the downstream traffic is not secure, and encrypting the downstream SIP (Session Initiation Protocol (https://en.wikipedia.org/wiki/Session_Initiation_Protocol)) transmission will not thwart stream

interception.

Spying on the doorbell allows for a gathering of sensitive information – household habits, names and details about family members, including children – all of which make the target easy prey for future exploitation. “Security is only as strong as its weakest link,” added Atias. “When handling sensitive data like a video doorbell, secure transmission is not a feature, but a must – particularly as the average consumer will not be aware of any tampering.”

The Ring video doorbell vulnerability was found during the process of routine ethical hacking where the Dojo by BullGuard cyber research team examines various IoT devices to constantly improve the Dojo Intelligent IoT Platform (DIP) capabilities to defend against potential vulnerabilities. Amazon has already released a new version of the Ring mobile app where this vulnerability has been fixed and the device is now safe from this kind of attack.

Read the full details of the Ring video doorbell vulnerability on the Dojo blog (https://dojo.bullguard.com/dojo-by-bullguard/blog/).

About BullGuard

BullGuard (https://www.bullguard.com/) is a multi-award winning, smart home cybersecurity company. We make it simple to protect everything in your digital life – from your data, to your identity, to your Smart Home. The BullGuard product portfolio extends to PCs, tablets and smartphone protection, and includes internet security, comprehensive mobile security, 24/7 identity protection and VPN which provides the highest levels of privacy and protection. BullGuard released the world’s first IoT vulnerability scanner and leads the consumer cybersecurity industry in providing continuous innovation.

Dojo by BullGuard (https://dojo.bullguard.com/) is an award-winning intelligent defense system and service that provides the highest level of protection to consumers across all of their connected devices and smart homes. Dojo by BullGuard is the cornerstone of a Smart Home, ensuring a connected world where every consumer in every home, is smart, safe and protected.

Follow us on Twitter @BullGuard (http://www.twitter.com/BullGuard) and @DojoSafe (http://www.twitter.com/DojoSafe), and like us on Facebook at BullGuard (https://www.facebook.com/BullGuard/?fref=ts) and Dojo (https://www.facebook.com/meetdojo/?fref=ts).

###

Media Contact:

Michelle Cross
The PR Room
michelle.cross@theprroom.co.uk