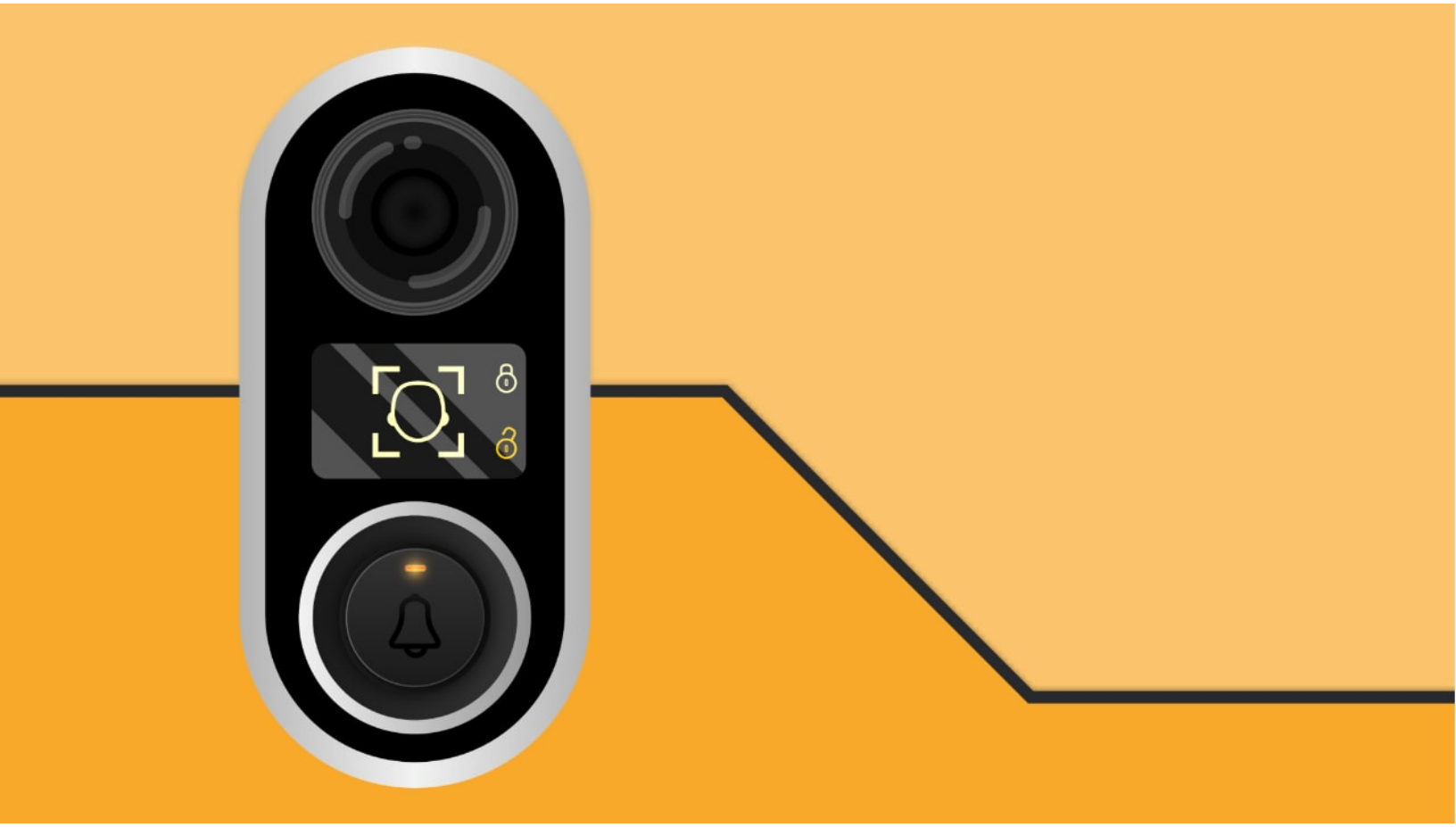
nccgroup



Nov 23, 2020 07:30 GMT

Smart doorbells – delivering the security you expect?

2020 has been the year of staying home, so it makes sense that we invest in the latest tech to keep it connected and running smoothly. Smart TVs, plugs, toys, cameras and doorbells are all being used to streamline our daily lives, but how secure are these devices?

For a long time, NCC Group has been committed to researching the security of the IoT ecosystem, not just for devices used within homes, but also across our workplaces, to understand the risks we're facing as an increasingly connected society.

Over the last year, our researchers have been working closely with independent UK consumer body, Which?, to delve into the security of smart consumer devices that are being used across our homes. In October, we released research into smart plugs which uncovered 13 security and safety issues across nine devices.

Since then, we've seen vendors rollout fixes and marketplaces take down affected products – a great result and the driver for research like this, but there's always more to be done. This is why we decided to look at the risks that eleven smart doorbells from lesser-known brands could pose to consumer security...

Findings: a digital spy-hole for cyber criminals?

During our assessment, we uncovered a wide variety of security issues relating to the hardware, associated mobile applications and the cloud servers which streamed and transferred data collected through the doorbells.

This included issues with the doorbell's insecure built-in Wi-Fi, which could leave sensitive information, such as credentials viewable in plaintext, to a remote attacker. Another device was vulnerable to KRACK – a critical vulnerability, which could allow an attacker to break the WPA-2 security on a Wi-Fi router, gaining access to their network.

However, the most worrying vulnerability we uncovered was related to the cloud servers and services used to transfer and store the data collected through the doorbells. From our assessment, we were able to identify several devices which connected to cloud-based servers outside of the UK and Europe, which can pose a big risk to consumer data.

In some cases, data streamed via or stored in servers in these locations included location data, photos, audio, video, email addresses and credentials such as usernames, passwords and Wi-Fi authentication details.

Who's responsible for IoT security?

Speaking on this research Matt Lewis, research director at NCC Group said: "Our findings could cause issues for consumers and are indicative of a wider culture that favors shortcuts over security in the manufacturing process.

"However, we are hopeful that a much-anticipated IoT legislation will signal a watershed moment for IoT security. Until this comes into fruition, we must continue to work together to highlight the need for basic security by design principles, and educate consumers about the risks and what they can to protect themselves."

But what can manufacturers do to address these issues while we await legislation that will set the bar for security across all IoT devices?

Our researchers highlighted a number of recommendations, including:

- Use modern and secure encryption – to prevent eavesdropping and to protect the integrity of data, encryption should be mandatory across all doorbells, mobile application storage and communication. This should include the data saved on the SD card or transferred between the doorbell and mobile application themselves, or over the public internet to the related cloud-based servers.
- Eliminate undocumented features – this would also prevent many of the issues we identified in this research. To put it simply, if a feature is not documented, it is of immediate interest to an attacker as it could be vulnerable and serve as a backdoor into the wider network.
- Enforce access control measures across all components – this will ensure that requests can only be performed as an authorised user or device owner.
- Provide adequate anti-tamper protection – When any hardware is outside a building, there is a risk of the device being unmounted from its bracket and stolen. Therefore, it's important that manufacturers work in adequate tamper protection to reduce the risk of theft as far as possible.

What can consumers do to protect themselves?

As we draw closer to the holiday season, more and more consumers will be looking for the latest IoT products for their homes, families and friends, but it's important to remain vigilant when making these purchases.

If you're unsure about what you need to be looking for, we have a handy guide on the simple things you can do to ensure you're purchasing a device

that will keep your information safe and secure, as well as mitigations you can put in place across your home and devices.

You can read the Which?
article here: https://www.which.co.uk/news/2020/11/the-smart-video-doorbells-letting-hackers-into-your-home/

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970