nccgroup

Royalty-free stock vector ID: 1523831471

Oct 01, 2020 10:52 BST

Lights out for smart plugs?

Our home environments are becoming increasingly connected – particularly with the help of smart plugs, which turn systems such as lighting or heating, into intelligent ones that allow consumers to run and monitor their homes at the click of a button on their phone or command through a smart speaker.

But how secure are these smart plugs, and what issues could they pose to consumer safety and security?

Working with leading UK independent consumer body, Which?, our researchers tested the security of ten smart plugs currently available on the market to see just how secure the devices were, and whether there were any issues that could lead to the compromise of the plugs or the appliances that are connected to them.

We carried out open source research for each smart plug, vulnerability research on the electronic interfaces and a teardown of the hardware layer, as well as an assessment of the mobile applications associated to the plugs, and privacy review to find out if devices were beaconing out information that could identify the user or device.

The findings…

Our testing uncovered 13 vulnerabilities in nine of the plugs that could pose risks to the safety and security of consumers.

Many of the issues identified came down to poor implementation and product development practices. This included weak encryption and plaintext transmission of network passwords, which could allow hackers to compromise the plugs, as well as products and devices connected to the plugs, including thermostats, camera or even a laptop.

On top of this, when taking one of the plugs apart, our team found a particularly worrying safety issue that couldcause a luminous electrical discharge between two electrodes – a significant fire risk, particularly for homes that have older wiring.

Pressing need for legislation

If this research highlights anything, it's the growing need for legislation to come into force to hold manufacturers to account and ensure basic principles of secure by design.

The good news though is that this research comes as the UK's Department for Digital, Culture, Media and Sport (DCMS) continues its call for evidence on legislation that will mandate three basic requirements for consumer Internet of Things (IoT) devices:

- Device passwords must be unique and not resettable to any universal factory setting
- Manufacturers must provide a public point of contact so anyone

can report a vulnerability
- Information stating the minimum length of time for which the device will receive security updates must be provided to customers

Although these requirements may seem basic, research like ours continues to show that manufacturers across the globe are failing to implement basic security principles into the devices they are producing, and as a result are putting consumer safety and security at risk.

While we await this much needed legislation, it’s important that consumers are doing what they can to ensure the smart plugs and devices they are buying are up to scratch when it comes safety and security. This includes:

- **Research the brand –** Doing some research on the brand you're purchasing from is an important first step. While an unknown manufacturer doesn't always suggest that a device is vulnerable, a well-known vendor is likely to have a better track record of fixing security or safety issues. Check to see if they have a basic internet presence, such as a vendor website.
- **Look out for fake kite marks –** Once you receive the product, it's good practice to check for any fake kite markings. If a product has been produced in China, it will have a CE mark, which stands for China Export, but this doesn't mean it has been tested by an authorised lab. To help distinguish between a China Export product and an EU tested product, check if the C lines up into the E. If the CE does not line up, it's likely that this is not sold in the EU and can be deemed a fake CE marking.
- **Change the default password –** This is one of the first things you should do when implementing any connected device in your home. National Cyber Security Centre (NCSC) guidance recommends creating a password that uses three random words.
- **Keep on top of updates –** Many of us are used to automatic updates on our phones or laptops, but not all devices do these automatically. Checking the settings for this will ensure that your devices have the latest software and security updates.

For more guidance on how to keep your connected devices safe at home, we’ve pulled together a handy infographic which you can find here.

If you’d like to take a technical deep dive into the research, check out our research blog in a couple of weeks.

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

NCC Group - Financial Media Enquiries
Press Contact
Maitland AMO
Financial Results Media Enquiries
+44 (0)20 7379 5151

Regional Press Office - North America
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750