Poison Ivy RAT Spotted in Three New Attacks - http://t.co/GhWUJBGSvx




- Tweet 0 Share on Twitter
- Share on Facebook
- Google +1 7
- Share 7 Share on LinkedIn


4


# Philips Light Bulb Vulnerability Could Leave Some In the Dark

by Chris Brook August 15, 2013 , 3:41 pm

According to research unveiled this week some types of web-enabled light bulbs are vulnerable to a flaw wherein an attacker could literally leave users of the bulbs in the dark.

Philips' Hue brand lighting systems can be exploited, according to independent researcher Nitesh Dhanjani who published a paper, Hacking Lightbulbs (.PDF) to accompany his research on Tuesday.

## Related Posts

**Poison Ivy RAT Spotted in Three New Attacks**

August 21, 2013 , 4:00 am

**NHTSA Servers Back Online After Attack**

August 13, 2013 , 3:57 pm

**Threatpost News Wrap, August 9, 2013**

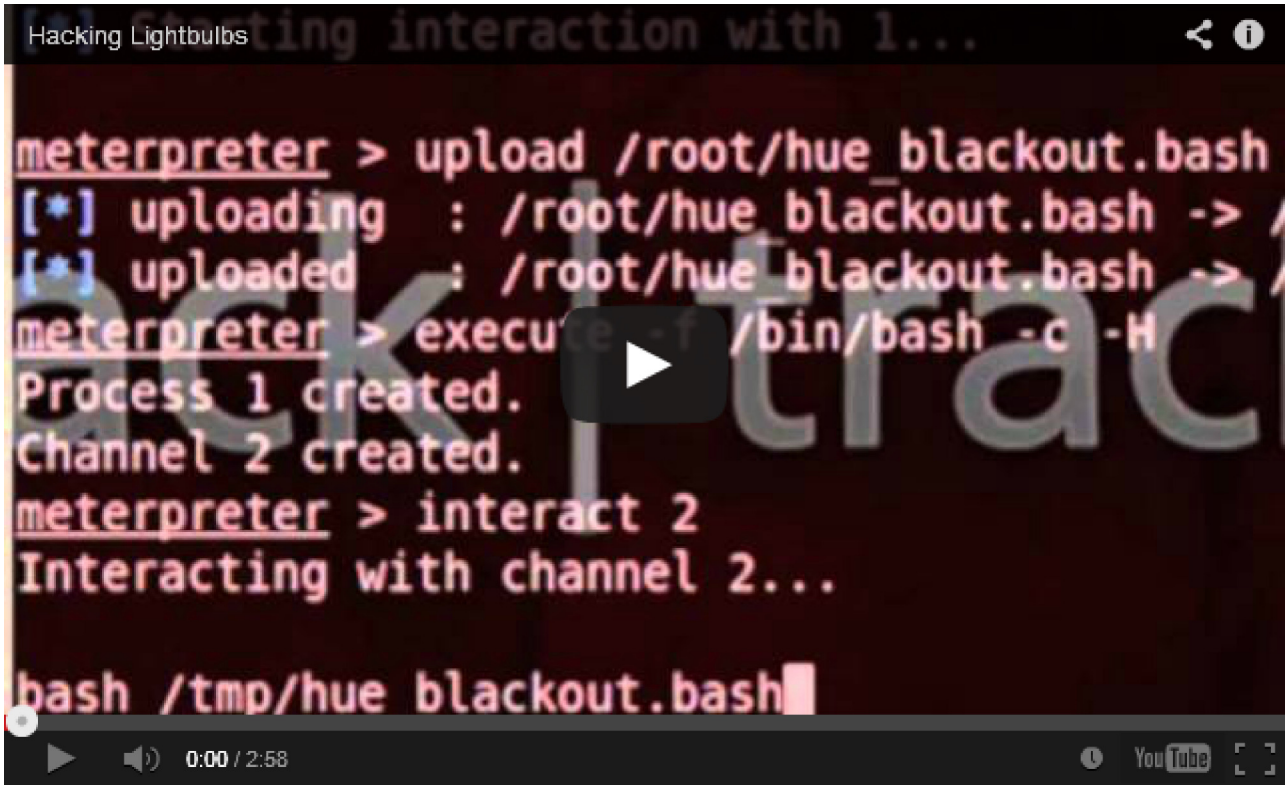
August 9, 2013 , 9:00 am

Hue received scattered acclaim last year after it popped up at the Apple store and was later called the best new product of 2012 by Forbes. Essentially it's a wireless system that can manage an infrastructure of LED light bulbs via iOS and Android devices.

The main problem here lies in the fact that Hue's bridge uses a whitelist of associated tokens to authenticate its requests. Anyone else who can get on its network and glean at least one of the whitelisted tokens can issue HTTP commands to the system and in turn control the lightbulbs.

Dhanjani notes that in testing, determining one of the whitelist tokens was not difficult, it was simply the MD5 hash of the MAC address of the users' iOS or Android device.

"This leaves open a vulnerability whereby malware on the internal network can capture the MAC address active on the wire (using the ARP cache of the infected machine). Once the malware has computer the MD5 of the captured MAC addresses, it can cycle through each hash and issue 'all lights off' instructions to the bridge via HTTP."




Attackers can repeatedly insert code to trigger a "sustained blackout," and rig the victim's system so they can remotely change people's light bulbs.

In one – perhaps farfetched situation – an attacker could even cause a blackout in a person's home or office just by tagging a completely black image of them on Facebook. This stems from functionality in the app that lets social media dictate users' lighting. Hue can change lights to reflect the color of an Instagram or Facebook photo and blink a certain number of times if they receive an email.

Dhanjani contacted the makers of the system, Philips, several times via Twitter in June to address the issues with Hue but the company never responded with an email to Dhanjani to further explain the vulnerability.

When reached this week Philips claimed it was aware of Dhanjani's whitepaper but insists the vulnerability is only possible on local area networks, adding that if users secure their internet, "traffic passing between your devices and across the internet will remain fully secure."

The news that an internet-connected lighting system is vulnerable shouldn't come as too big of a surprise. In this day in age – as we've learned with cars, pacemakers, washing machines and even coffee makers – practically everything that can connect to the internet can be compromised.

While Dhanjani warns "lighting is critical to physical security," and that if anyone were to exploit this vulnerability in a hospital or public venue, it could cause trouble, it's not likely many of these vulnerabilities will really affect the general public. In advertising, the product is catered more towards the home and in most situations it's hard to comprehend being left in the dark as anything more than just a nuisance.


- Tweet 0 Share on Twitter
- Share on Facebook
- Google +1 +1 7
- Share 7 Share on LinkedIn


4
Categories: Hacks, Vulnerabilities

# Comments (4)

1. *Ralph* August 15, 2013 @ 10:14 pm
   1

   I am developing a lightbulb which can operate 100% autonomously, without any internet connection. My product will revolutionize home security. Eventually I hope to get the price low enough to compete with ordinary internet bulbs. Until then, it will be available as a high-end product for those who require, and can afford, a higher level of protection.

   Reply ↓

   - *Jose* August 16, 2013 @ 4:50 pm
     2

     Great! Best of Luck!

     Reply ↓
2. *Nicola* August 16, 2013 @ 4:15 pm
   3

   Ralph, I feel your research is very important. I have been working on a completely Internet free light bulb for about a year now. I feel we should exchange notes for the betterment of mankind. Please contact me in the near future.

   Reply ↓
3. *T* August 16, 2013 @ 5:05 pm
   4

   @Ralph: Perfect comment – You win the internet today!!

Reply ↓

### Leave A Comment

Your email address will not be published. Required fields are marked *

Name *

Email *

Comment

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <strike> <strong>`

Post Comment

☐ Notify me of follow-up comments by email.

☐ Notify me of new posts by email.

## Recommended Reads

- Tweet 0 Share on Twitter
- Share on Facebook
- Google +1 +1 4
- Share 2 Share on LinkedIn

0
August 21, 2013 , 4:00 am
Categories: Malware

### Poison Ivy RAT Spotted in Three New Attacks

by Michael Mimoso

Researchers have spotted the Poison Ivy RAT being used in three new attacks with ties to China.