

Synack Report, Company Comments

Kidde (products: Kidde Smoke Detector)

Thank you for contacting us. Kidde's mission is to develop solutions that protect people from fire and its related hazards. Although we haven't seen the actual Synack study referenced, we're pleased with the results we've seen in media coverage, which indicate that our product received a perfect score from a security perspective.

Kidde offers a range of smoke alarms including those that feature sealed long-life batteries, hardwired with interconnected capabilities, and wireless notification both inside and outside the home. Kidde continuously explores new ways to use technology to address real issues and consumer needs and trends, while maintaining the integrity of the mission of our products.

Heather Caldwell

Kidde Fire Safety

SmartThings (products: SmartThing Home Automation Controller)

Protecting customer's privacy and data securely are fundamental to everything we do at SmartThings. We regularly perform penetration tests of our system and engage companies doing White Hat testing on a continuous basis to improve the quality and security of our products. When vulnerabilities are identified we address them immediately and are transparent with our customers about our efforts.

On background and not for attribution, it may be important to note that Synack has provided a summary

BREW
MEDIA RELATIONS

Caitlyn Carpanzano

Vice President

Nest (products: the Nest smoke detectors, thermostats, home automation controller by Resolv and cameras by Dropcam)

- ALL hardware devices - from laptops to smartphones (e.g. iPhones) - are susceptible to hacking with physical access. This is called a jailbreak. (For what it's worth, once someone has access to your home, chances are they would install their own devices, or take the jewelry. :))
- The hack by Synack was a jailbreak.
- What's important is that a jailbreak doesn't compromise the security of our servers or the connections to them and to the best of our knowledge, no Nest devices have been accessed and compromised remotely.

The last point I'd like to make - which you may already be aware of from speaking with Synack - is that Nest products were the most secure in the categories that Synack tested.

Ha Thai

Nest Communications

ArcSoft (products: Simplicam Camera)

Thanks so much for providing us with the opportunity to comment. While we have been made aware of the report through another outlet that wrote about it, it was not made available to us, nor have we been able to locate it anywhere online or otherwise.

From what I gather from the article, it seems to be speculation that Simplicam was wirelessly hacked: "Colby Moore, a security research analyst who compiled the report, said it took him about 20 minutes to break into each of the assorted devices." We have found no proof that Simplicam was wirelessly hacked, and find it surprising we would be indirectly accused without proof. In addition, **there are facts stated in a grid from a previous article that are inaccurate**, and we appreciate the opportunity to correct them:

- We [encourage consumers to use safe password practices](#). We would also like to point out that Simplicam does NOT have a default password; we require users to set up an account password precisely to encourage security measures.

- If the user attempts to add a Simplicam to a non-secure, non-password protected Wi-Fi network, they will see a message encouraging them not to do so, as it is unsafe.

- Only one account can access a camera. Unlike competitors, no camera is allowed to stream live to the public, for security and privacy reasons.

- It is **factually incorrect** that we have "no certificate validation at whatsoever" (sic). We use Symantec certificate validation.

-In addition to layers of proprietary encryption, we use Amazon web services for our cloud hosting, which adds yet another layer of its own security requirements.

Based on this information and without being able to locate an actual “report”, we are forced to question the credibility of the source. We are happy to introduce you to industry analysts unassociated with any home monitoring products, such as Parks & Associates or Forrester Research, for further commentary on best practices and the smart home.

Caroline Tien-Spalding

Senior Director, Marketing

ArcSoft www.arcsoft.com

Honeywell (products: Lyric Thermostat)

Home security is the top concern for both Honeywell and our customers, which is why we design every connected thermostat with security in mind. We’ve reached out to the researcher behind this study to better understand his findings, and to ensure we continue to meet the high standards that our customers rightfully expect from us.

Thanks again for reaching out to us on this!

Mark Hamel

Honeywell

Automation and Control Solutions

Control 4 (products: Control4 Home Automation Controller)

Thank you for getting in contact with us on this topic.

The security and privacy of our customers is a top priority for Control4 and we always strive to employ industry best practices. Security will always be a concern in the industry and it's something that will continue to evolve. That's why we're dedicated to providing education and tools for both our expert installers and consumers to help them understand these issues and be vigilant when it comes to securing a smart home.

--

Blair Sonnen, PR Manager

Control4 |

Withings (products: Withings Camera)

"Withings takes security very seriously. As Synack noted in their report, Home's software can be updated remotely with very little effort from the end user. We always recommend users to use complex passwords and an ethernet connection can be used for extra security. Also, through DTLS, we ensure data is securely transmitted all along the way from the device to the smartphone. We are very open to getting more details from Synack on their tests and are contacting them to get further understanding their results." Alexis Fabre Ringborg, Chief Operations Officer.

Ecobee (products: Ecobee Thermostat)

It's difficult to comment on the validity of the Synack report as they have not released the details of the report to us and it's unclear how Synack arrived at their conclusions. What I can say is that ecobee takes customer privacy and security very seriously. ecobee has deep security expertise, we implement industry best practices and we use many of the same encryption and authentication technologies used, and depended upon, by millions of people everyday, for internet banking and e-commerce transactions.

Kind regards,

Tenille Kennedy

Director Communication

Ecobee

Lowe's Iris Home Automation Controller

No response by deadline

Hive British Gas (Hive Thermostat)

No response by deadline

Foscam (Foscam Camera)

No response by deadline

First Alert (Smoke Detector)

No response by deadline