Confirmed: 2 Billion Records Exposed In Massive Smart Home Device Breach!

By Davey Winder July 2, 2019

NWC ALLIANCE · FRIDAY, JULY 26, 2019 · 6 MINUTES

Confirmed: 2 Billion Records Exposed In Massive Smart Home Device Breach

NWC ALLIANCE · FRIDAY, JULY 26, 2019 · 6 MINUTES

A team of self-styled "hacktivist" security researchers, with an impressive track record of exposing breach after breach as part of a web-mapping project that searches for vulnerabilities within online databases, has disclosed one of the biggest to date. The researchers in question, Noam Rotem and Ran Locar from vpnMentor, found that a user database belonging to a Chinese company called Orvibo, which runs an Internet of Things (IoT) management platform, had been left exposed to the Internet without any password to protect it. So far, so appalling. But it gets even worse when you discover that the database includes more than 2 billion logs containing everything from user passwords to account reset codes and even a "smart" camera recorded conversation.

Who is Orvibo?

Orvibo is a Chinese company based in Shenzhen, from where it operates a smart home device management platform. The Orvibo website boasts of a secure cloud providing a "reliable smart home cloud platform," and goes on to mention how it "supports millions of IoT devices and guarantees the data safety." I imagine that the vpnMentor researchers might well take issue with that given how the breach methodology itself was shockingly predictable: a misconfigured and Internet-facing Elasticsearch database without a password. Just to add salt to the wound, a Kibana web-based app that makes navigating through the data contained in that database easier was also left with no password protection. Geoff Tudor, general manager of Vizion.ai, told me that Elasticsearch breaches are becoming almost everyday occurrences. "When first installed, Elasticsearch's API is completely open without any password protection," Tudor says, adding "all a hacker needs to do is to hit a URL with http://[serverIP]:9200 and a user can see if an Elasticsearch is operational. Then it takes a single command to search through the data stored in it..."

Less salt in the wound

The list of data included in the breach is extensive according to the vpnMentor report and includes:

- Email addresses
- Passwords

- Account reset codes
- Precise geolocation
- IP address
- Username
- UserID
- Family name
- Family ID
- Smart device
- Device that accessed account
- Scheduling information

Of these, the most problematical are the password and password reset codes that are being logged. Even though these had not been encrypted, they had been hashed using MD5. Unlike encryption, which is a two-way function in that it is designed so you can decrypt the data at some point, hashing is a one-way thing that isn't reversible. Hashing turns a plaintext password into a unique hexadecimal string, it's an authentication thing, a check-sum if you like. Unfortunately, the MD5 algorithm used to hash these passwords isn't considered particularly secure as it has been found to contain a whole bunch of vulnerabilities. The Orvibo incident went one step further when it comes to diluting the security value of MD5 hashing: the passwords and reset codes were hashed but not salted. By adding a unique value, or salt, to the end of every password before hashing you produce a different hash value. This additional security layer is vital if you want to protect against a brute force attack that tries every known alphanumeric combination until the password is revealed. Rainbow tables, lists of hashes and their corresponding passwords, can also be made much less likely to succeed if every hashed password has a unique salt.

What could attackers do with this data?

Given that Orvibo claims to have more than a million users, including private individuals with smart home systems but also hotels and other business customers, the implications are quite far reaching. Orvibo manufactures some 100 different smart home or smart automation devices. The vpnMentor report states that it found logs for users in China, Japan, Thailand, Mexico, France, Australia, Brazil, the United Kingdom and the U.S.

According to the researchers, the reset codes were the most dangerous pieces of information found in the database. "These would be sent to a user to reset either their password or their email address," the report explains, continuing "with that information readily accessible, a hacker could lock a user out of their account without needing their password. Changing both a password and an email address could make the action irreversible."

But that's just the tip of this incident iceberg, given that a number of home security devices are included in the Orvibo product line. These include smart locks, home security cameras and full smart home kits. "With the information that has leaked," the report says, "it's clear that there is nothing secure about these devices. Even having one of these devices installed could undermine, rather than enhance, your physical security."

"Misconfigurations that leave servers open and vulnerable is something that we've seen resurface over and over again," Ben Herzberg, director of threat research at Imperva, told me. "When these systems are left open attackers have a variety of options, they can either use the data to their advantage, take over resources," Herzberg continued, concluding "or work themselves even further into the networks of the organization and infiltrate additional resources."

What can you do to secure your smart device data?

"Criminal groups may have been aware of this vulnerability but it is unknown if anyone has taken advantage of this flaw yet," says Jake Moore, a cybersecurity specialist at ESET who adds, "I'd hope it would be patched quite quickly now it is out." That hope seems like a bit of a reach to me considering that vpnMentor says it first contacted Orvibo on June 16 without response. It then tweeted the company, but this didn't get any response either. As of yesterday, ZDNet reports that despite continued efforts to contact the company not only has there been no response but the database remains freely accessible online with no password protection.

"The best thing now for people affected is to make sure their smart device passwords are changed immediately to something long and complex along with other accounts where the same password may be reused," Moore advises. However, he also points out that if cyber-criminal gangs are already in and watching their every move before a patch is installed, "they may as well pull the plug on the device until it is fixed."

Ilia Kolochenko, founder and CEO of web security company ImmuniWeb, concludes that beyond the obvious password changing, users of Orvibo devices have little recourse "but to file a legal complaint and deactivate any remote management of their homes if it is doable."

July 4, 2019.

An Orvibo spokesperson has provided the following comment:

"Once we received this report on July 2, Orvibo's RD team took immediate actions *to resolve security vulnerability and informed the reporter. Orvibo attaches great importance to user data security and keeps improving information security systems."*

I can also confirm that the Orvibo database in question has been closed as of July 2.

NWC Alliance

Nwcalliance.com

https://www.forbes.com/sites/daveywinder/2019/07/02/confirmed-2-billion-records-exposed-in-massive-smart-home-device-breach/?fbclid=IwAR1obiNiBE4uXnviKg3gUe-n9gflfTA2z2fmzgF66jdMOoa4rtd1-n72CIo#7235d41c411c