IOActive Security Advisory

Title	Petcube Remote Wireless Pet Camera Vulnerabilities
Severity	Critical
Discovered by	Mike Davis
Advisory Date	April 10, 2015

Affected Products

1. Petcube Remote Wireless Pet Camera

Impact

The security and privacy of Petcube users could be compromised.

Background

Internet of Things (IoT) device maker, Petcube, produces a line of cloud-accessible pet monitoring cameras which allow owners to access cameras, send and receive audio, and control a connected laser peripheral. IOActive has discovered multiple security issues with Petcube's security model which could allow unauthorized access.

Technical Details

1) Petcube devices primarily use RSYNC over SSH to collect device information and provide firmware updates. To accomplish this, Petcube distributes two distinct SSH private keys for the users "logger" and "updater" which are shared by all Petcube users. This method provides no effective isolation between user logging facilities.

2) Petcube's server-side security is based on a script "rsync.sh" which is configured as the logger/updater shell and appears to be based on this web page (http://troy.jdmz.net/rsync/index.html). This approach to rsync does not appear to provide any security and can be overwritten by any Petcube user by providing one of multiple paths to command execution allowed by this configuration.

3) Petcube alternately uses a TLS certificate to communicate over HTTPS to Petcube cloud services. This TLS private key is also shared by all Petcube devices, allowing an attacker the ability to sniff or act as a MitM.

4) SSH/RSYNC-based firmware upgrades are further compromised by the addition of the SSH flag:
`-o StrictHostKeyChecking=no`. When combined with the exposure of the private key, this allows a MitM on firmware upgrades.

5) The MySQL to EBS Backup password (and script) is world readable.

Fixes

None at this time.

Timeline

- February 18, 2015: IOActive discovers vulnerability
- March 3, 2015: IOActive notifies vendor
- April 10, 2015: IOActive advisory published
- April 12, 2015: Vendor released new firmware addressing reported vulnerabilities

