rippleLabs

Gateway Bulletin GB-2015-04 Action Required : Default Ripple Flag
Subject : Important Patch : Potential Rippling Vulnerability Fixed.

March 13, 2015

Contents

Overview

Ripple Labs has patched a vulnerability involving the No Ripple (also known as rippling) flag. Previously, it was possible for an attacker to shift a target account's balance from higher value assets to lower value assets of the same type. For example, if you held multiple issues of USD that did not trade at parity, it was possible for the attacker to shift higher value USD in exchange for lower value USD (even if the user had not enabled rippling).

To correct this issue, a new flag has been added to accounts that explicitly enables rippling. Gateways should enable this flag to allow their users to make payments to each other. Most users should leave this flag disabled to prevent the unintentional shifting of funds. The required actions for gateways and users as described below.

The vulnerability, which potentially affected about 7% of Ripple Trade users, was reported on March 8 and was patched by Ripple Labs 3 days later.

[Action Required] by Users

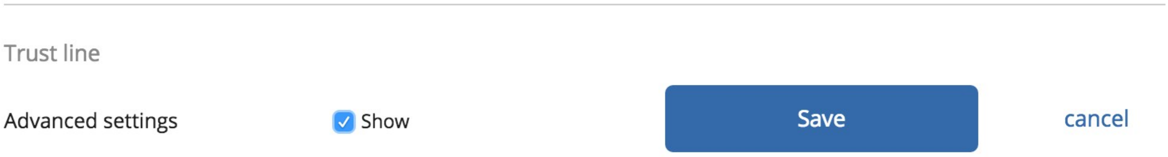
How to Enable NoRipple in Ripple Trade

If you hold multiple gateway balances of the same currency, your settings may currently allow your balances to shift between gateways. In particular, although the total balance remains the same, the balances may shift. For example, if you have $100 SnapSwap USD and $50 Bitstamp USD, without any action on your part, you could end up with $0 SnapSwap USD and $150 Bitstamp USD. If you don't want your gateway funds to potentially shift, you should follow the instructions below.

<u>Action required to prevent gateway balance shifting</u>

To prevent your balances from unitentionally shifting, you should examine your gateways (also known as trust lines) and ensure all your trust lines have Rippling off (Rippling is what enables balances to shift).

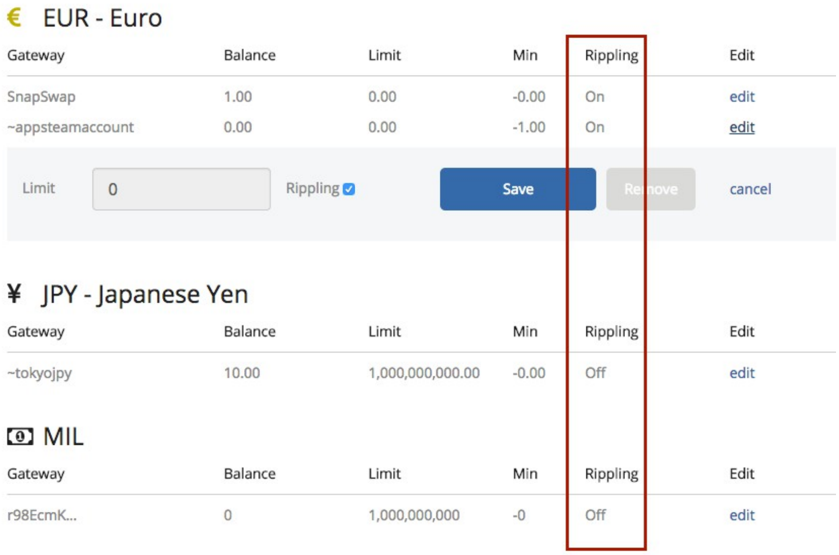
1) Navigate to the Settings gear (top right) > Settings > Advanced and check "Show" for trust line advanced settings.



Trust line

Advanced settings ☑ Show

2) Go back to the Fund tab > Gateways page.
Under the "Rippling" column, you'll want to make sure all gateways (both incoming and outgoing) have Rippling off. To turn Ripple off, click **Edit > Uncheck the "Rippling" box > Save**.



€ EUR - Euro

Gateway	Balance	Limit	Min	Rippling	Edit
SnapSwap	1.00	0.00	-0.00	On	edit
~appsteamaccount	0.00	0.00	-1.00	On	edit

Limit 0 Rippling ☑

¥ JPY - Japanese Yen

Gateway	Balance	Limit	Min	Rippling	Edit
~tokyojpy	10.00	1,000,000,000.00	-0.00	Off	edit

MIL

Gateway	Balance	Limit	Min	Rippling	Edit
r98EcmK...	0	1,000,000,000	-0	Off	edit

Now none of your balances will be able to shift between gateways.

How to Enable NoRipple on an Incoming trust line using rippled

For users that do not manage their Ripple wallet with Ripple Trade, a TrustSet transaction is required to enable the NoRipple flag. An example call is :

```
curl -k -H 'Content-Type: application/json' -X POST -d '{
 "method" : "sign",
 "params" : [ {
   "offline" : true,
   "secret" : <account_secret>,
   "tx_json" : {
     "Flags":"131072",
     "Fee": "15000",
     "TransactionType":"TrustSet",
     "Account":"<account_public>",
     "LimitAmount": {
       "currency" : "<set_appropriately>",
       "value":"0",
       "issuer" : "<account_that_trusted_you>"
     },
     "Sequence": "<next_sequence_number>"
   }
} ]
}' https://localhost:5005
```

Of course, you must provide the correct values for your situation:

- account_secret - The secret key of the issuing account
- Account - The Ripple address of the issuing account
- issuer field of LimitAmount - The address of the account that extended trust to you
- value field of LimitAmount - Must be zero
- LastLedgerSequence - 4 higher than the most recent ledger_index
    - Optional, and not recommended for offline signing

To perform offline signing, you must also provide:

- Fee - appropriate for current network fees
- Sequence - Your account’s next sequence number

The result of this transaction is a signed tx_blob that you can submit to any rippled server without exposing your secret. For example, to submit to the Ripple Labs public cluster:

```
curl -X POST -d '{
        "method" : "submit",
        "params" : [ {
                "tx_blob" : "1200002280000000002400. . . "
        }]
}' http://s1.ripple.com:51234
```

[Action Required] by Gateway Operators

Gateways must update their rippled servers to at least rippled version 0.27.3-sp1. Gateways should also use the newly added noripple_check RPC command to check for accounts that have been affected by an edge case that can occur with the patch.

Update Local rippled Server and Enable DefaultRipple Flag

The patch requires all rippled servers in the network to upgrade. The latest updated rippled branch has been tagged and is located at :

https://github.com/ripple/rippled/tree/0.27.3-sp2

Additionally, gateway cold wallets must set the asfDefaultRipple flag on a rippled version 0.27.3-sp1 (or later) server to resume normal operations. To set the flag, you may issue the following command to a local rippled server :

```
$ ./rippled submit cold_wallet_secret '{
    "Account" : "cold_wallet_public",
    "TransactionType" : "AccountSet",
    "SetFlag" : 8
}'
```

Please use security best practice by not submitting cold wallet secret keys to any untrusted rippled server, including the Ripple Labs public cluster s1.ripple.com.

Check for Edge Case Trust Lines

There is an edge case window between March 10th at 4:26 PM and when the gateway has set the asfDefaultRipple flag.

Without this flag set, payments will fail between users whose trust lines were established to the gateway during the edge case window unless action is taken as described below. To assist in identifying these edge cases, Ripple Labs has provided a tool to display required action. See below.

For each trust line established during the edge case window, a gateway must issue a TrustSet, for limit zero, and clear the NoRipple flag. If you cannot perform this manually in Ripple Trade, you can use a curl command to a local rippled server, such as:

```
curl -k -H 'Content-Type: application/json' -X POST -d '{
 "method" : "sign",
 "params" : [ {
   "offline" : true,
   "secret" : <account_secret>,
   "tx_json" : {
     "Flags":"262144",
     "Fee": "15000",
     "TransactionType":"TrustSet",
     "Account":"<account_address>",
     "LimitAmount": {
       "currency" : "<set_appropriately>",
       "value":"0",
       "issuer" : "<account_that_trusted_you>"
     },
     "Sequence": "3"
   }
} ]}' https://localhost:5005
```

You must provide the correct values for your situation:

- account_secret - The secret key of the issuing account.
- Account - The Ripple address of the issuing account.
- issuer field of LimitAmount - The address of the account that extended trust to you.
- value field of LimitAmount - Must be zero.
- LastLedgerSequence (Optional) - 4 higher than the most recent ledger_index. Not recommended for offline signing.

To perform offline signing, you must also provide:

- Fee - appropriate for current network fees
- Sequence - Your account's next sequence number

The result of this transaction is a tx_blob that you may submit to any rippled server. For example, to submit to the Ripple Labs public cluster:

```
curl -X POST -d '{
        "method" : "submit",
        "params" : [ {
                "tx_blob" : "12000022800000002400. . . "
        }]
}' http://s1.ripple.com:51234
```

Tool to Check for Edge Cases

Ripple Labs has created a tool to help gateways assess what they need to do to resume normal operations. We've added the noripple_check RPC command. This helps gateways make the changes needed to adjust to the "default ripple" flag. The noripple_check RPC command tells gateways how to set the "default ripple" flag and fixes any trust lines created before the gateway set the flag.

Once your server is running and synchronized, you can run the tool from the command line:

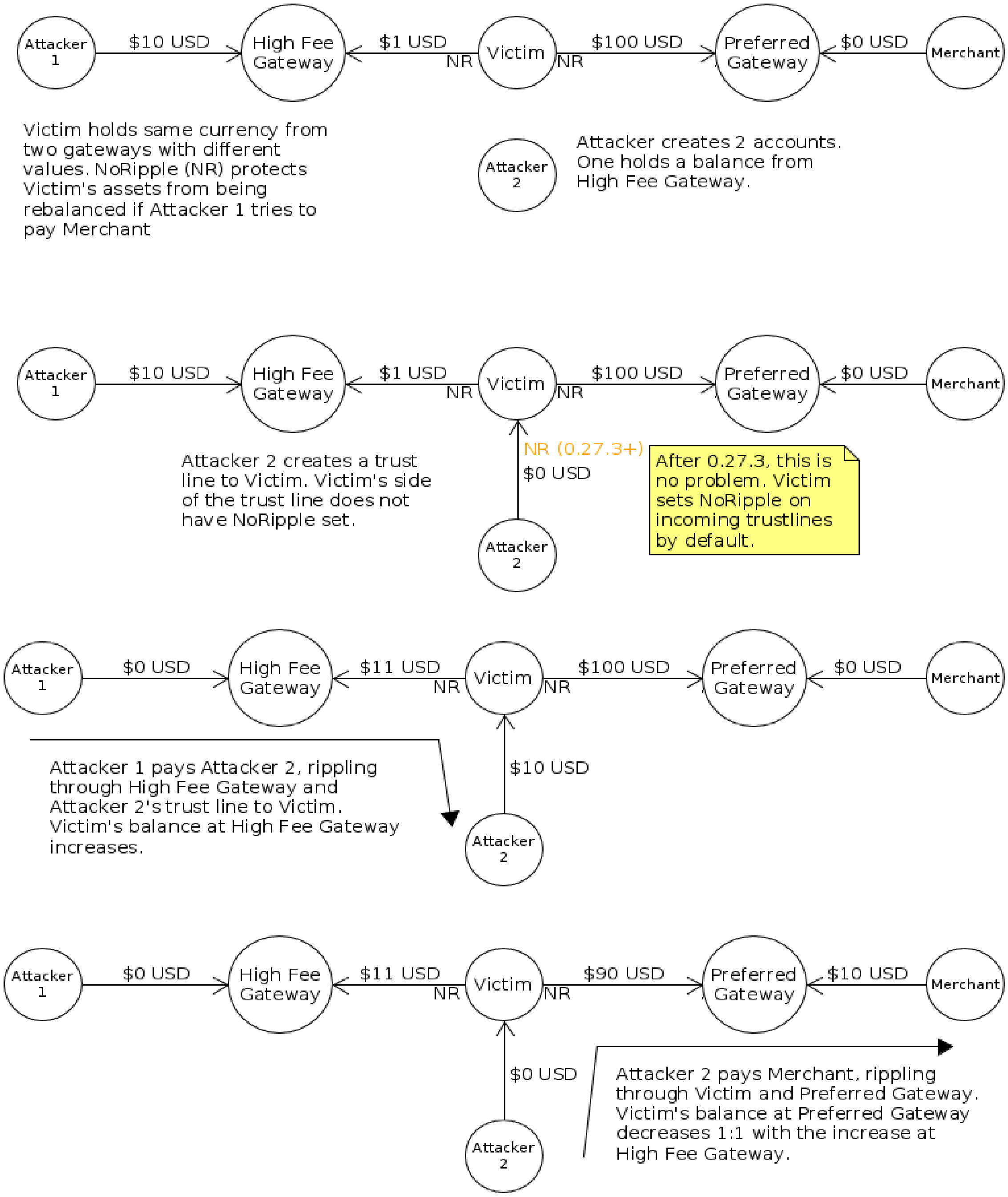
```
 $ ./rippled json noripple_check '
  {
    "account" : "<gateway_trusted_address_here>",
    "role" : "gateway",
    "transactions" : "true"
  }'
```

The server will respond with a list of problems with the configuration of the account and its trust lines. It will also return a transactions array suggesting the transactions needed to fix the problems it found.

Here is an example of the tool’s output:

```
"result" : {
   "ledger_index" : 12202269,
   "problems" : [
      "You should immediately set your default ripple flag",
      "You should clear the no ripple flag on your BTC line to rfTiZ53FW6aXcY9TFXQbZMsHQeP4h6Dgkh",
      "You should clear the no ripple flag on your BTC line to rQJDk9q5cLmiRYgeYxagsNekaiymTa9fXN"
   ],
   "status" : "success",
   "transactions" : [
      {
         "Account" : "rvYAfWj5gh67oV6fW32ZzP3Aw4Eubs59B",
         "Fee" : 10000,
         "Sequence" : 663,
         "SetFlag" : 8,
         "TransactionType" : "AccountSet"
      },
      {
         "Account" : "rvYAfWj5gh67oV6fW32ZzP3Aw4Eubs59B",
         "Fee" : 10000,
         "Flags" : 262144,
         "LimitAmount" : {
            "currency" : "BTC",
            "issuer" : "rfTiZ53FW6aXcY9TFXQbZMsHQeP4h6Dgkh",
            "value" : "0"
         },
         "Sequence" : 664,
         "TransactionType" : "TrustSet"
      },
      {
         "Account" : "rvYAfWj5gh67oV6fW32ZzP3Aw4Eubs59B",
         "Fee" : 10000,
         "Flags" : 262144,
         "LimitAmount" : {
            "currency" : "BTC",
            "issuer" : "rQJDk9q5cLmiRYgeYxagsNekaiymTa9fXN",
            "value" : "0"
         },
         "Sequence" : 665,
         "TransactionType" : "TrustSet"
      },
            ],
   "validated" : true
```

Taking advantage of this vulnerability required specific circumstances.



Victim holds same currency from two gateways with different values. NoRipple (NR) protects Victim's assets from being rebalanced if Attacker 1 tries to pay Merchant

Attacker creates 2 accounts. One holds a balance from High Fee Gateway.

Attacker 2 creates a trust line to Victim. Victim's side of the trust line does not have NoRipple set.

After 0.27.3, this is no problem. Victim sets NoRipple on incoming trustlines by default.

Attacker 1 pays Attacker 2, rippling through High Fee Gateway and Attacker 2's trust line to Victim. Victim's balance at High Fee Gateway increases.

Attacker 2 pays Merchant, rippling through Victim and Preferred Gateway. Victim's balance at Preferred Gateway decreases 1:1 with the increase at High Fee Gateway.

After the release of rippled version 0.27.3-sp1 on March 10, 2015, it is no longer possible to create those circumstances. However, accounts that were already in a position where their assets can be rebalanced (because the attacker has a trust line without NoRipple enabled from the victim's side) are still vulnerable. To fix the problem, the account should enable NoRipple on any incoming trust lines that existed prior to March 10, 2015.

Do not hesitate to contact Ripple Labs with questions at support@ripple.com.

Finally, Ripple Labs sends kind thanks to Martin Kreidenweis for responsibly reporting this vulnerability and working with us to help protect Ripple users.

Security related bugs can always be reported to support@ripple.com.