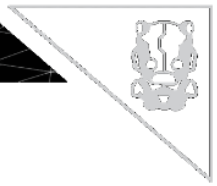
IOActive
Research-fueled Security Services

Code Review and Penetration Test

Pando Inc.

IOActive, Inc.
1426 Elliott Ave W
Seattle, WA 98119

Toll free: (866) 760-0222
Office: (206) 784-4313
Fax: (206) 784-4367



Document Management

Document Information

Client Name	Pando Inc.
Project Name	Pando Code Review and Penetration Test
Initial Project	2021-06-07 – 2021-07-02
Retest	2021-08-09

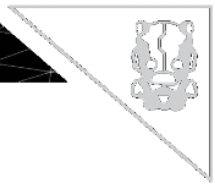
Document Revision Information

Date	Version	Author	Revision Details
2021-08-11	1.0	IOActive	Initial Version
2021-08-13	1,1	Roy Albert	Director Review
2021-08-27	1.2	IOActive	Updates

Project Contacts

IOActive, Inc.

Name	Title	Contact Information
Pablo Sisca	Security Consultant	pablo.sisca@ioactive.com
Roy Albert	Director of Services	roy.albert@ioactive.com
Shelby Green	Senior Engagement Manager	shelby.green@ioactive.com



Contents

Executive Summary 1

Project Description 1

Analysis of Findings 2

Detailed Findings 3

#MP-07 - Compound - Borrow Repayment Transaction May Fail After Modifying Borrow Balance [FIXED] 3

#MP-06 - Outdated Web Server with Multiple Vulnerabilities [FIXED] 9

#MP-01 - Lack of Certificate Pinning 16

#MP-02 - Insufficient Jailbreak Detection 17

#MP-03 - App Transport Security Disabled 19

#MP-04 - RPATH Set in Binary 21

#MP-05 - Binary Uses Insecure APIs 24

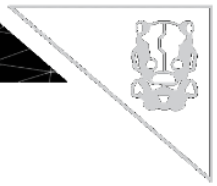
Appendix A: Overview of Risk Ratings and Finding Tables 26

Risk Ratings 26

Finding Descriptors 27

Finding Categories 28

Appendix B: Scope 29



Executive Summary

Pando Inc. (Pando) engaged IOActive, Inc. (IOActive) to assess the security threats and risks associated with its Pando service. Pando is a decentralized financial network built using Mixin Trusted Group (MTG) technology, a multi-signature, custodian-consensus solution. Its underlying financial algorithm is inspired by MakerDao and Synthetix.

Project Description

Three IOActive consultants conducted the assessment from the 7th of June to the 2nd of July 2021 for a total effort of eight resource weeks. The consultants focused on the test priorities discussed during the kick-off call, including reviewing the Mixin Messenger iOS app and its interaction with the MTG technology framework as well as the most common web application security vulnerabilities as listed in the OWASP Top Ten.

The following branches were in scope for this assessment:

- https://github.com/fox-one/compound/tree/audit
- https://github.com/fox-one/pando/tree/audit

The consultants paid particular attention to business logic found within the following areas of the codebase:

- Pando:
  - pkg/maker
  - worker/assigner
  - worker/cashier
  - worker/payee
  - worker/syncer
- Compound:
  - Key code: https://github.com/fox-one/compound/tree/audit/worker
  - Business logic: https://github.com/fox-one/compound/tree/audit/worker/snapshot

Subsequently, Pando engaged IOActive to perform remediation validation testing of select findings. One IOActive consultant retested two findings on the 9th of August 2021.

Analysis of Findings

Figure 1 shows the distribution of findings by risk rating.

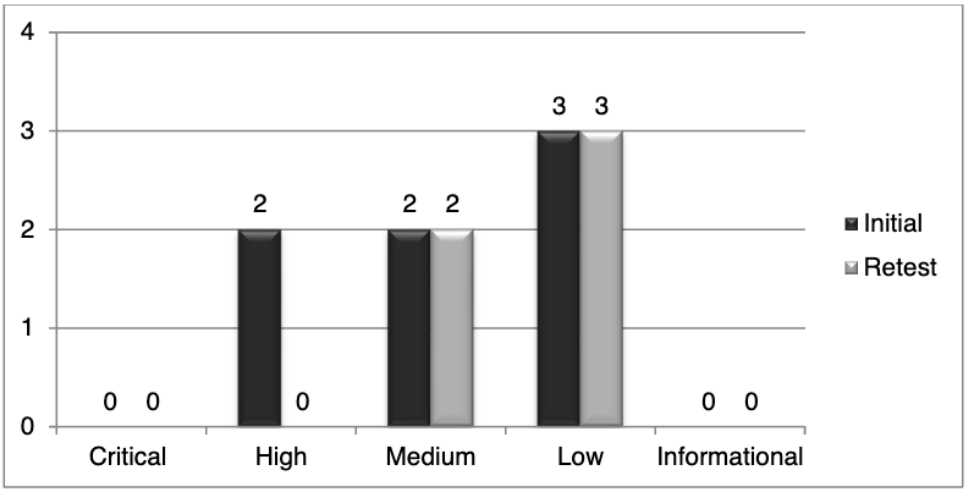


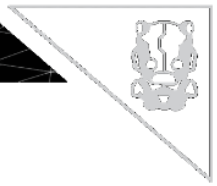
Figure 1. Distribution of Findings

In July 2021, IOActive reported two high-risk, two medium-risk, and three low-risk vulnerabilities in the Pando service.

In August 2021, IOActive retested the high-risk vulnerabilities and confirmed they were both properly fixed.

Table 1. Remediation status

Finding ID	Title	Total Risk	Status
#MP-07	Compound - Borrow Repayment Transaction May Fail After Modifying Borrow Balance	High	Fixed
#MP-06	Outdated Web Server with Multiple Vulnerabilities	High	Fixed
#MP-01	Lack of Certificate Pinning	Medium	
#MP-02	Insufficient Jailbreak Detection	Medium	
#MP-03	App Transport Security Disabled	Low	
#MP-04	RPATH Set in Binary	Low	
#MP-05	Binary Uses Insecure APIs	Low	



Detailed Findings

#MP-07 - Compound - Borrow Repayment Transaction May Fail After Modifying Borrow Balance [FIXED]

Host(s) / File(s)	Compound worker/snapshot/borrow_repay.go
Category	Authentication
Testing Method	Code Review
Tools Used	Visual Studio Code
Likelihood	Medium (3)
Impact	Critical (5)
Total Risk Rating	High (15)
Remediation Status	Fixed
Effort to Fix	Low

Threat and Impact

IOActive found that the borrow repayment logic in `Payee.handleRepayEvent()` suffered from a logic bug that could result in a 'borrow balance' being updated as 'repaid' or 'partially repaid' in the event of edge case failure conditions. As such, the error exists because logic within this function updates the balance on the relevant `borrow` object before actually generating and storing the transactions necessary for the repayment to take place. If error conditions occur during the system's attempts to generate and store these transactions, the result will be that the borrow would appear to have been repaid, yet no repayment transactions will end up taking place.

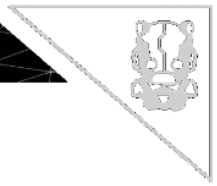
The discussion below briefly outlines the relevant code path.

The `payee` worker in Compound is responsible for dispatching handling for a number of events, including `ActionTypeRepay`. This action is used to repay a `borrow` (i.e. a loan). When an item of this type is encountered by the worker, Compound calls into `Payee.handleRepayEvent()`, which lives in the `worker/snapshot/borrow_repay.go` file.

The code fragments below, from `Payee.handleRepayEvent()`, show the relevant borrow balance being updated, with failure conditions actually being possible after these updates are made. Note the annotations of the form "`[n] potential failure point`."

```
//update borrow info
      borrowBalance, e := w.borrowService.BorrowBalance(ctx,
borrow, market)
      if e != nil {
```

```
            log.Errorln(e)
            return e
      }
      realRepaidBalance := repayAmount
      redundantAmount :=
repayAmount.Sub(borrowBalance).Truncate(8)
      newBalance := borrowBalance.Sub(repayAmount)
      newIndex := market.BorrowIndex
      if newBalance.LessThanOrEqual(decimal.Zero) {
            newBalance = decimal.Zero
            newIndex = decimal.Zero
            realRepaidBalance = borrowBalance
      }

      if output.ID > borrow.Version {
            borrow.Principal = newBalance.Truncate(16)
            borrow.InterestIndex = newIndex.Truncate(16)
            if e = w.borrowStore.Update(ctx, borrow,
output.ID); e != nil {     // [1] update the 'borrow' with
the new balance that is correct after the user-specified
amount is deducted due to repayment
                  log.Errorln(e)
                  return e
            }
      }

....

      if output.ID > market.Version {
            market.TotalBorrows =
market.TotalBorrows.Sub(realRepaidBalance).Truncate(16)
            market.TotalCash =
market.TotalCash.Add(realRepaidBalance).Truncate(16)
            if e = w.marketStore.Update(ctx, market,
output.ID); e != nil {    // [2] potential failure point
                  log.Errorln(e)
                  return e
            }
      }

      // market transaction
      marketTransaction :=
core.BuildMarketUpdateTransaction(ctx, market,
foxuuid.Modify(output.TraceID, "update_market"))
      if e = w.transactionStore.Create(ctx,
marketTransaction); e != nil {     // [3] potential failure
point
            log.WithError(e).Errorln("create transaction
error")
            return e
      }

      // add transaction
      extra := core.NewTransactionExtra()
      extra.Put(core.TransactionKeyBorrow, core.ExtraBorrow{
            UserID:        borrow.UserID,
```



```
            AssetID:       borrow.AssetID,
            Principal:     borrow.Principal,
            InterestIndex: borrow.InterestIndex,
      })
      transaction := core.BuildTransactionFromOutput(ctx,
userID, followID, core.ActionTypeRepay, output, extra)
      if e = w.transactionStore.Create(ctx, transaction); e
!= nil {       // [4] potential failure point
            log.WithError(e).Errorln("create transaction
error")
            return e
      }
```

The operation at [1] updates the 'borrow balance' as per the amount the user is attempting to repay (e.g. complete or partial balance), and this change is committed to the 'borrow store'. However, failure points exist at [2], [3], and [4]; if failure does happen at one of these points, transactions to actually repay the 'borrow' may not actually be created in the system, hence the 'borrow' will appear to have been repaid, yet repayment will not actually happen.

These operations at these failure points revolve around database commit operations, with the relevant 'stores' being SQLite databases managed by the GORM library. Whilst failures at these points may be unlikely under normal operating conditions, simple database commit operations may occasionally fail under high load or when a system experiences edge-case conditions; for example, low memory conditions may result in memory allocation failures, which in turn could result in a database commit operation failing overall.

Recommendations

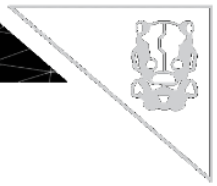
Commit changes to the borrow store only after generating and storing the relevant repayment transactions.

Retest Results

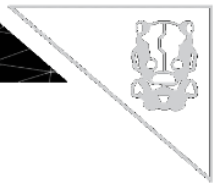
2021-08-09: Fixed

The code now makes sure that the database is not updated if the payment fails.

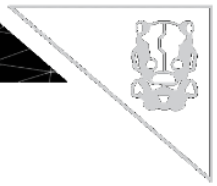
```
// handle borrow repay event
func (w *Payee) handleRepayEvent(ctx context.Context, output
*core.Output, userID, followID string, body []byte) error {

   log := logger.FromContext(ctx).WithField("worker",
"borrow_repay")

   repayAmount := output.Amount
   assetID := output.AssetID

   log.Infoln(":asset:", output.AssetID, "amount:",
repayAmount)

   market, e := w.marketStore.Find(ctx, assetID)
   if e != nil {
         return e
```



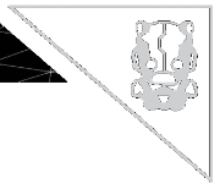
```
    }

    if market.ID == 0 {
          return w.handleRefundEvent(ctx, output, userID,
followID, core.ActionTypeRepay, core.ErrMarketNotFound)
    }

    //update interest
    if e = w.marketService.AccrueInterest(ctx, market,
output.CreatedAt); e != nil {
          log.Errorln(e)
          return e
    }

    borrow, e := w.borrowStore.Find(ctx, userID, market.AssetID)
    if e != nil {
          return e
    }

    if borrow.ID == 0 {
          return w.handleRefundEvent(ctx, output, userID,
followID, core.ActionTypeRepay, core.ErrBorrowNotFound)
    }

    transaction, e := w.transactionStore.FindByTraceID(ctx,
output.TraceID)
    if e != nil {
          return e
    }

    if transaction.ID == 0 {
          if w.marketService.IsMarketClosed(ctx, market) {
                return w.handleRefundEvent(ctx, output, userID,
followID, core.ActionTypeRepay, core.ErrMarketClosed)
          }

          //update borrow info
          borrowBalance, e := w.borrowService.BorrowBalance(ctx,
borrow, market)
          if e != nil {
                log.Errorln(e)
                return e
          }

          newBalance := borrowBalance.Sub(repayAmount)
          newIndex := market.BorrowIndex
          if !newBalance.IsPositive() {
                newBalance = decimal.Zero
                newIndex = decimal.Zero
                repayAmount = borrowBalance
          }
```



```
        extra := core.NewTransactionExtra()
        extra.Put("repay_amount", repayAmount.Truncate(16))
        extra.Put("new_balance", newBalance.Truncate(16))
        extra.Put("new_index", newIndex.Truncate(16))
        extra.Put(core.TransactionKeyBorrow, core.ExtraBorrow{
              UserID:        borrow.UserID,
              AssetID:       borrow.AssetID,
              Principal:     newBalance,
              InterestIndex: newIndex,
        })

        transaction = core.BuildTransactionFromOutput(ctx,
userID, followID, core.ActionTypeRepay, output, extra)
        if e := w.transactionStore.Create(ctx, transaction); e
!= nil {
              return e
        }
   }

   var extra struct {
        RepayAmount decimal.Decimal `json:"repay_amount"`
        NewBalance  decimal.Decimal `json:"new_balance"`
        NewIndex    decimal.Decimal `json:"new_index"`
   }

   if e := transaction.UnmarshalExtraData(&extra); e != nil {
        return e
   }

   if output.ID > borrow.Version {
        borrow.Principal = extra.NewBalance
        borrow.InterestIndex = extra.NewIndex
        if e = w.borrowStore.Update(ctx, borrow, output.ID); e
!= nil {
              log.Errorln(e)
              return e
        }
   }

   if refundAmount := output.Amount.Sub(extra.RepayAmount);
refundAmount.GreaterThan(decimal.Zero) {
        transferAction := core.TransferAction{
              Source:   core.ActionTypeRepayRefundTransfer,
              FollowID: followID,
        }

        if e := w.transferOut(ctx, userID, followID,
output.TraceID, assetID, refundAmount, &transferAction); e !=
nil {
              return e
        }
   }
```



```
    if output.ID > market.Version {
          market.TotalBorrows =
market.TotalBorrows.Sub(extra.NewBalance).Truncate(16)
          market.TotalCash =
market.TotalCash.Add(extra.NewBalance).Truncate(16)
          if e = w.marketStore.Update(ctx, market, output.ID); e
!= nil {
                log.Errorln(e)
                return e
          }
    }

    return nil
}
```



#MP-06 - Outdated Web Server with Multiple Vulnerabilities [FIXED]

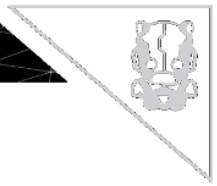
Host(s) / File(s)	api.mixin.one:443 mixin-api.zeromesh.net:443
Category	Software Vulnerabilities
Testing Method	Black Box
Tools Used	Burp Suite
Likelihood	Medium (3)
Impact	High (4)
Total Risk Rating	High (12)
Remediation Status	Fixed
Effort to Fix	Low

Threat and Impact

The web server is running an outdated version of Nginx. Using out-of-date software increases the risk of using code that has known vulnerabilities that have since been patched. Based on the banner reported by the web server, the current version used has multiple vulnerabilities that potentially could be exploited remotely; no attempt was made to do so.

- CVE-2019-9511 - 7.8 - Some HTTP/2 implementations are vulnerable to window size manipulation and stream prioritization manipulation, potentially leading to a denial of service.
- CVE-2018-16844 - 7.8 - Nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage.
- CVE-2019-9513 - 7.8 - Some HTTP/2 implementations are vulnerable to resource loops, potentially leading to a denial of service.
- CVE-2019-9516 - 6.8 - Some HTTP/2 implementations are vulnerable to a header leak, potentially leading to a denial of service.
- CVE-2018-16843 - 7.8 - Nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption.
- CVE-2018-16845 - 5.8 - Nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure.

```
GET https://api.mixin.one/
```



```
HTTP/2 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Mon, 14 Jun 2021 16:16:57 GMT
...
```

```
GET https://mixin-api.zeromesh.net/

HTTP/2 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Mon, 07 Jun 2021 16:22:47 GMT
...
```

Recommendations

Upgrade to the latest version of the web server.

Additional Information

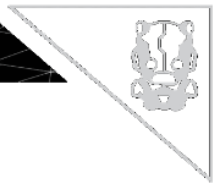
Nginx security advisories: https://nginx.org/en/security_advisories.html

Retest Results

2021-08-09: Fixed

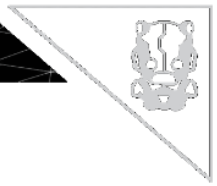
Fingerprints cannot be obtained from either affected server, as shown below.

```
$ curl -v https://api.mixin.one
*   Trying 35.201.113.166...
* TCP_NODELAY set
* Connected to api.mixin.one (35.201.113.166) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/cert.pem
  CApath: none
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-CHACHA20-POLY1305
* ALPN, server accepted to use h2
* Server certificate:
*  subject: CN=*.mixin.one
*  start date: Oct 14 00:00:00 2020 GMT
```



```
*  expire date: Nov 14 23:59:59 2021 GMT
*  subjectAltName: host "api.mixin.one" matched cert's
"*.mixin.one"
*  issuer: C=GB; ST=Greater Manchester; L=Salford; O=Sectigo
Limited; CN=Sectigo RSA Domain Validation Secure Server CA
*  SSL certificate verify ok.
* Using HTTP2, server supports multi-use
* Connection state changed (HTTP/2 confirmed)
* Copying HTTP/2 data in stream buffer to connection buffer
after upgrade: len=0
* Using Stream ID: 1 (easy handle 0x7fce7d80d600)
> GET / HTTP/2
> Host: api.mixin.one
> User-Agent: curl/7.64.1
> Accept: */*
>
* Connection state changed (MAX_CONCURRENT_STREAMS == 100)!
< HTTP/2 200
< server: nginx
< date: Sat, 07 Aug 2021 07:47:00 GMT
< content-type: application/json; charset=UTF-8
< content-length: 157
< x-build-info: a9ccef1df34e125b723ebbb42e601891a88c8445-go1.16
< x-request-id: 9c7cedfb-3bd5-4846-a7a6-6f1c6260aa37
< x-runtime: 0.002756
< x-server-time: 1628322420617397814
< via: 1.1 google
< alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-
T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-
Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443";
ma=2592000; v="46,43"
<
* Connection #0 to host api.mixin.one left intact
{"data":{"build":"a9ccef1df34e125b723ebbb42e601891a88c8445-
go1.16","developers":"https://developers.mixin.one","timestamp"
:"2021-08-07T07:47:00.617352392Z"}}* Closing connection 0
```

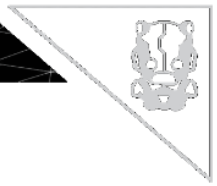
```
$ curl -v https://mixin-api.zeromesh.net/
*   Trying 34.117.37.130...
* TCP_NODELAY set
* Connected to mixin-api.zeromesh.net (34.117.37.130) port 443
(#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/cert.pem
  CApath: none
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
```



```
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-CHACHA20-POLY1305
* ALPN, server accepted to use h2
* Server certificate:
*  subject: CN=*.zeromesh.net
*  start date: Dec  8 00:00:00 2020 GMT
*  expire date: Dec  8 23:59:59 2021 GMT
*  subjectAltName: host "mixin-api.zeromesh.net" matched cert's
"*.zeromesh.net"
*  issuer: C=GB; ST=Greater Manchester; L=Salford; O=Sectigo
Limited; CN=Sectigo RSA Domain Validation Secure Server CA
*  SSL certificate verify ok.
* Using HTTP2, server supports multi-use
* Connection state changed (HTTP/2 confirmed)
* Copying HTTP/2 data in stream buffer to connection buffer
after upgrade: len=0
* Using Stream ID: 1 (easy handle 0x7fde4500d600)
> GET / HTTP/2
> Host: mixin-api.zeromesh.net
> User-Agent: curl/7.64.1
> Accept: */*
>
* Connection state changed (MAX_CONCURRENT_STREAMS == 100)!
< HTTP/2 200
< server: nginx
< date: Sat, 07 Aug 2021 07:47:54 GMT
< content-type: application/json; charset=UTF-8
< content-length: 157
< x-build-info: a9ccef1df34e125b723ebbb42e601891a88c8445-go1.16
< x-request-id: fe2ccd53-ce20-4642-81c9-b219a8b9abb6
< x-runtime: 0.001622
< x-server-time: 1628322474412252073
< via: 1.1 google
< alt-svc: clear
<
* Connection #0 to host mixin-api.zeromesh.net left intact
{"data":{"build":"a9ccef1df34e125b723ebbb42e601891a88c8445-
go1.16","developers":"https://developers.mixin.one","timestamp"
:"2021-08-07T07:47:54.412221678Z"}}* Closing connection 0
```

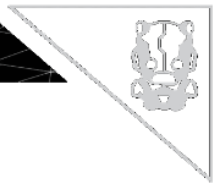
```
$ sudo nmap -sV -A -p80,443 mixin-api.zeromesh.net
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-07 08:48 BST
Nmap scan report for mixin-api.zeromesh.net (34.117.37.130)
Host is up (0.032s latency).
Other addresses for mixin-api.zeromesh.net (not scanned):
34.117.59.206
```

```
rDNS record for 34.117.37.130:
130.37.117.34.bc.googleusercontent.com

PORT    STATE SERVICE  VERSION
80/tcp  open  http
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.0 404 Not Found
|     Content-Type: text/html; charset=UTF-8
|     Referrer-Policy: no-referrer
|     Content-Length: 1561
|     Date: Sat, 07 Aug 2021 07:48:55 GMT
|     <!DOCTYPE html>
|     <html lang=en>
|     <meta charset=utf-8>
|     <meta name=viewport content="initial-scale=1, minimum-
scale=1, width=device-width">
|     <title>Error 404 (Not Found)!!1</title>
|     <style>
|_    *{margin:0;padding:0}html,code{font:15px/22px arial,sans-
serif}html{background:#fff;color:#222;padding:15px}body{margin:
7% auto 0;max-width:390px;min-height:180px;padding:30px 0
15px}* >
body{background:url(//www.google.com/images/errors/robot.png)
100% 5px no-repeat;padding-right:205px}p{margin:11px 0
22px;overflow:hidden}ins{color:#777;text-decoration:none}a
img{border:0}@media screen and (max-
width:772px){body{background:none;margin-top:0;max-
width:none;padding-
right:0}}#logo{background:url(//www.google.com/images/branding/
googlelogo/1x/goo
|_http-title: Error 404 (Not Found)!!1
443/tcp open  ssl/http nginx
|_http-title: Site doesn't have a title (application/json;
charset=UTF-8).
| ssl-cert: Subject: commonName=*.zeromesh.net
| Subject Alternative Name: DNS:*.zeromesh.net,
DNS:zeromesh.net
| Not valid before: 2020-12-08T00:00:00
|_Not valid after:  2021-12-08T23:59:59
|_ssl-date: 2021-08-07T07:49:58+00:00; 0s from scanner time.
| tls-alpn:
|   grpc-exp
|   h2
|_  http/1.1
| tls-nextprotoneg:
|   grpc-exp
|   h2
|_  http/1.1
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
```

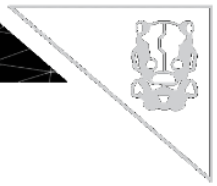


```
No OS matches for host
```

```
$ sudo nmap -sV -A -p80,443 api.mixin.one
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-07 08:50 BST
Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing
Service Scan
Service scan Timing: About 50.00% done; ETC: 08:52 (0:00:54
remaining)
Nmap scan report for api.mixin.one (35.201.113.166)
Host is up (0.052s latency).
Other addresses for api.mixin.one (not scanned): 130.211.45.251
rDNS record for 35.201.113.166:
166.113.201.35.bc.googleusercontent.com

PORT    STATE SERVICE  VERSION
80/tcp  open  http
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.0 404 Not Found
|     Content-Type: text/html; charset=UTF-8
|     Referrer-Policy: no-referrer
|     Content-Length: 1561
|     Date: Sat, 07 Aug 2021 07:50:58 GMT
|     <!DOCTYPE html>
|     <html lang=en>
|     <meta charset=utf-8>
|     <meta name=viewport content="initial-scale=1, minimum-
scale=1, width=device-width">
|     <title>Error 404 (Not Found)!!1</title>
|     <style>
|_    *{margin:0;padding:0}html,code{font:15px/22px arial,sans-
serif}html{background:#fff;color:#222;padding:15px}body{margin:
7% auto 0;max-width:390px;min-height:180px;padding:30px 0
15px}* >
body{background:url(//www.google.com/images/errors/robot.png)
100% 5px no-repeat;padding-right:205px}p{margin:11px 0
22px;overflow:hidden}ins{color:#777;text-decoration:none}a
img{border:0}@media screen and (max-
width:772px){body{background:none;margin-top:0;max-
width:none;padding-
right:0}}#logo{background:url(//www.google.com/images/branding/
googlelogo/1x/goo
|_http-title: Error 404 (Not Found)!!1
443/tcp open  ssl/http nginx
|_http-title: Site doesn't have a title (application/json;
charset=UTF-8).
| ssl-cert: Subject: commonName=*.mixin.one
| Subject Alternative Name: DNS:*.mixin.one, DNS:mixin.one
| Not valid before: 2020-10-14T00:00:00
|_Not valid after:  2021-11-14T23:59:59
|_ssl-date: 2021-08-07T07:52:04+00:00; +1s from scanner time.
```



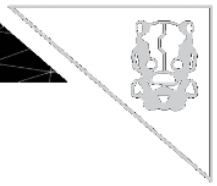
```
| tls-alpn:
|   grpc-exp
|   h2
|_  http/1.1
| tls-nextprotoneg:
|   grpc-exp
|   h2
|_  http/1.1
1 service unrecognized despite returning data.

OS and Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 74.06 seconds
```



#MP-01 - Lack of Certificate Pinning

Host(s) / File(s)	Mixin Messenger (iOS)
Category	Insecure Communication
Testing Method	Black Box
Tools Used	Smartphone, Burp Proxy
Likelihood	Low (2)
Impact	High (4)
Total Risk Rating	Medium (8)
Effort to Fix	Medium

Threat and Impact
Certificate pinning is the process of validating that the host being contacted via TLS/SSL presents the certificate expected by the application. In practice, this is typically implemented by embedding information about the certificate (usually the hash of the certificate's Subject Public Key Information fields) into the application. The application can compare the embedded, known good information with that of the presented certificate chain. The goal of certificate pinning is to prevent the application from accepting certificates that may validate but are actually fraudulent.
Recommendations
Implement certificate pinning in the app. Because the application will have to be updated when pins change, consider carefully the operational impact of implementing pinning in each application.
Additional Information
The OWASP guide to certificate and public key pinning: https://owasp.org/www-community/controls/Certificate_and_Public_Key_Pinning The CERT guide to properly verify server certificate on SSL/TLS: https://www.securecoding.cert.org/confluence/pages/viewpage.action?pageId=134807561 TrustKit Framework for iOS and Android: • https://github.com/datatheorem/TrustKit/ • https://github.com/datatheorem/TrustKit-Android

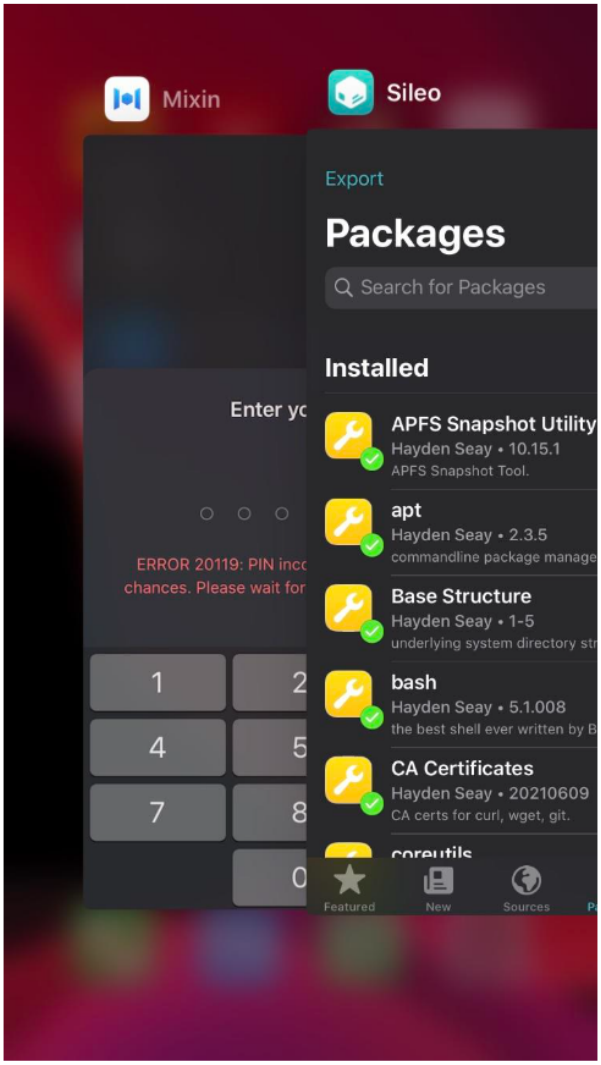


#MP-02 - Insufficient Jailbreak Detection

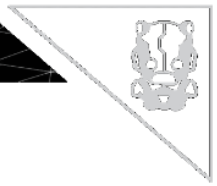
Host(s) / File(s)	Mixin Messenger (iOS)
Category	Configuration
Testing Method	Manual
Tools Used	iOS, Odyssey jailbreak
Likelihood	Medium (3)
Impact	Low (2)
Total Risk Rating	Medium (6)
Effort to Fix	Low

Threat and Impact
Once a device is jailbroken, some new files may be placed on the device. Checking for those files and packages installed on the device is one way of finding out if a device is jailbroken or not. Some developers may execute the commands which are accessible only to root users, and some may look for directories with elevated permissions. It's important to mention that in a jailbroken phone or emulator the user has full control of the device and therefore any checks performed in the device could be bypassed. Nevertheless, it is recommended to improve the jailbroken detection methods by including more granular sanity checks. Also, any attempt to use the application in a jailbroken environment should be alerted and if possible, the device should be blacklisted from the back end by using any unique identifier taken from the phone. Many iOS apps do not run on jailbroken devices for security reasons.

It was possible to install and run the app on a jailbroken iPhone. he screenshot below shows the Mixin Messenger app running alongside the Sileo jailbreak package manager on an iPhone 8 (iOS 13.5.1), jailbroken using Odyssey.



Recommendations
Perform checks that detect if the installation device has been jailbroken. Do not permit the app to run on jailbroken devices.
Additional Information
Techniques for jailbreak detection: https://www.cryptomathic.com/news-events/blog/application-hardening-for-mobile-banking-apps-root-and-jailbreak-detection



#MP-03 - App Transport Security Disabled

Host(s) / File(s)	Mixin Messenger (iOS)
Category	Insecure Communication
Testing Method	Manual
Tools Used	Mobile Security Framework (MobSF)
Likelihood	Low (2)
Impact	Low (2)
Total Risk Rating	Low (4)
Effort to Fix	Low

Threat and Impact

On Apple platforms, a networking feature called App Transport Security (ATS) improves privacy and data integrity for all apps and app extensions. ATS requires that all HTTP connections made with the URL Loading System-typically using the `URLSession` class-use HTTPS. It further imposes extended security checks that supplement the default server trust evaluation prescribed by the TLS protocol. ATS blocks connections that fail to meet minimum security specifications.

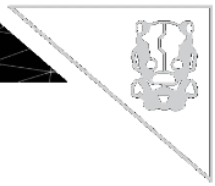
In the app, ATS restrictions were disabled for requests made from WebViews without affecting `URLSession` connections. This setting is not applicable to domains listed in `NSExceptionDomains`.

In `Info.plist`:

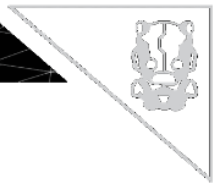
```
...
        <key>NSAppTransportSecurity</key>
        <dict>

<key>NSAllowsArbitraryLoadsInWebContent</key>
                <true/>
        </dict>
...
```

Recommendations

Use ATS to secure network connections as intended. If one or more exceptions are required, then add them explicitly to the configuration as described in Additional Information below.



Additional Information
Background: https://developer.apple.com/documentation/bundleresources/information_property_list/nsapptransportsecurity Preventing Insecure Network Exceptions: https://developer.apple.com/documentation/security/preventing_insecure_network_connections



#MP-04 - RPATH Set in Binary

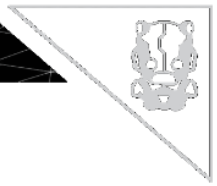
Host(s) / File(s)	Mixin Messenger (iOS)
Category	Configuration
Testing Method	Manual
Tools Used	otool
Likelihood	Low (2)
Impact	Low (2)
Total Risk Rating	Low (4)
Effort to Fix	Low

Threat and Impact

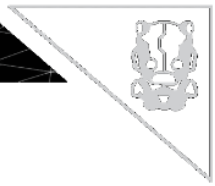
The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation.

The `otool` command can display specified parts of object files or libraries. It was used in this case to show where rpath had been utilized.

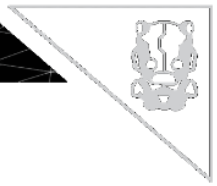
```
otool -l Mixin | grep rpath
name @rpath/AcknowList.framework/AcknowList (offset 24)
name @rpath/Alamofire.framework/Alamofire (offset 24)
name
@rpath/AlignedCollectionViewFlowLayout.framework/AlignedColl
ectionViewFlowLayout (offset 24)
name @rpath/DeviceGuru.framework/DeviceGuru (offset 24)
name @rpath/FBLPromises.framework/FBLPromises (offset 24)
name @rpath/FirebaseABTesting.framework/FirebaseABTesting
(offset 24)
name @rpath/FirebaseCore.framework/FirebaseCore (offset 24)
name
@rpath/FirebaseCoreDiagnostics.framework/FirebaseCoreDiagnos
tics (offset 24)
name
@rpath/FirebaseCrashlytics.framework/FirebaseCrashlytics
(offset 24)
name
@rpath/FirebaseInstallations.framework/FirebaseInstallations
(offset 24)
name
@rpath/FirebasePerformance.framework/FirebasePerformance
(offset 24)
```



```
name
@rpath/FirebaseRemoteConfig.framework/FirebaseRemoteConfig
(offset 24)
name @rpath/GRDB.framework/GRDB (offset 24)
name
@rpath/GoogleDataTransport.framework/GoogleDataTransport
(offset 24)
name @rpath/GoogleUtilities.framework/GoogleUtilities
(offset 24)
name @rpath/Gzip.framework/Gzip (offset 24)
name @rpath/Lottie.framework/Lottie (offset 24)
name @rpath/PhoneNumberKit.framework/PhoneNumberKit (offset
24)
name @rpath/Protobuf.framework/Protobuf (offset 24)
name @rpath/RSKImageCropper.framework/RSKImageCropper
(offset 24)
name @rpath/Rswift.framework/Rswift (offset 24)
name @rpath/SDWebImage.framework/SDWebImage (offset 24)
name @rpath/SDWebImageYYPlugin.framework/SDWebImageYYPlugin
(offset 24)
name @rpath/SQLCipher.framework/SQLCipher (offset 24)
name @rpath/SnapKit.framework/SnapKit (offset 24)
name @rpath/SocketRocket.framework/SocketRocket (offset 24)
name @rpath/YYImage.framework/YYImage (offset 24)
name @rpath/Zip.framework/Zip (offset 24)
name
@rpath/libsignal_protocol_c.framework/libsignal_protocol_c
(offset 24)
name @rpath/nanopb.framework/nanopb (offset 24)
name @rpath/openssl.framework/openssl (offset 24)
name @rpath/WebRTC.framework/WebRTC (offset 24)
name @rpath/libswiftAVFoundation.dylib (offset 24)
name @rpath/libswiftCallKit.dylib (offset 24)
name @rpath/libswiftContacts.dylib (offset 24)
name @rpath/libswiftCore.dylib (offset 24)
name @rpath/libswiftCoreAudio.dylib (offset 24)
name @rpath/libswiftCoreFoundation.dylib (offset 24)
name @rpath/libswiftCoreGraphics.dylib (offset 24)
name @rpath/libswiftCoreImage.dylib (offset 24)
name @rpath/libswiftCoreLocation.dylib (offset 24)
name @rpath/libswiftCoreMedia.dylib (offset 24)
name @rpath/libswiftDarwin.dylib (offset 24)
name @rpath/libswiftDispatch.dylib (offset 24)
name @rpath/libswiftFoundation.dylib (offset 24)
name @rpath/libswiftIntents.dylib (offset 24)
name @rpath/libswiftMapKit.dylib (offset 24)
name @rpath/libswiftMediaPlayer.dylib (offset 24)
name @rpath/libswiftMetal.dylib (offset 24)
name @rpath/libswiftObjectiveC.dylib (offset 24)
name @rpath/libswiftPhotos.dylib (offset 24)
name @rpath/libswiftQuartzCore.dylib (offset 24)
name @rpath/libswiftUIKit.dylib (offset 24)
name @rpath/libswiftsimd.dylib (offset 24)
```



Recommendations
Remove the compiler option `-rpath` to remove @rpath.
Additional Information
General background: https://en.wikipedia.org/wiki/Rpath RPATH exploitation: https://medium.com/@donblas/fun-with-rpath-otool-and-install-name-tool-e3e41ae86172



#MP-05 - Binary Uses Insecure APIs

Host(s) / File(s)	Mixin Messenger (iOS)
Category	Configuration
Testing Method	Manual
Tools Used	otool
Likelihood	Low (2)
Impact	Low (2)
Total Risk Rating	Low (4)
Effort to Fix	Low

Threat and Impact

The binary may contain the following insecure or deprecated APIs: `_strlen`, `_stat`, `_chmod`, `_sscanf`, `_memcpy`, `_printf`, and `_fopen`. Additionally, a weak random number generator was referenced, as were insecure hashing functions.

`otool` output:

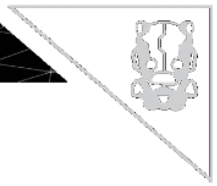
```
0x00000001008d121c  2102 _chmod
0x0000000100a58728  2102 _chmod
0x00000001008d2128  2509 _strlen
0x0000000100a59130  2509 _strlen
0x00000001008d20ec  2504 _stat
0x0000000100a59108  2504 _stat
0x00000001008d20e0  2503 _sscanf
0x0000000100a59100  2503 _sscanf
0x00000001008d17f8  2306 _memcpy
0x0000000100a58b10  2306 _memcpy
0x00000001008d1ab0  2366 _printf
0x0000000100a58ce0  2366 _printf
0x00000001008d1594  2176 _fopen
0x0000000100a58978  2176 _fopen
```

Weak random number generator also referenced:

```
0x00000001008d1c30  2398 _rand
0x0000000100a58de0  2398 _rand
```

Weak hash functions referenced:

```
0x00000001008d0610  1345 _CC_SHA1
0x0000000100a57f20  1345 _CC_SHA1
```



```
0x00000001008d0604  1344 _CC_MD5
0x0000000100a57f18  1344 _CC_MD5
```

Recommendations

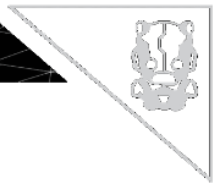
In general, code quality issues can be avoided by doing the following:

- Maintain consistent coding patterns that everyone in the organization agrees upon.
- Write code that is easy to read and well-documented.
- When using buffers, always validate that the lengths of any incoming buffer data will not exceed the length of the target buffer.
- Via automation, identify buffer overflows and memory leaks through the use of third-party static analysis tools.
- Prioritize solving buffer overflows and memory leaks over other 'code quality' issues.

The level of risk is dependent on how these functions are used, so review code to ensure that they are not involved in handling sensitive or otherwise critical data.

Additional Information

OWASP Top 10: M7: Client Code Quality https://owasp.org/www-project-mobile-top-10/2016-risks/m7-client-code-quality



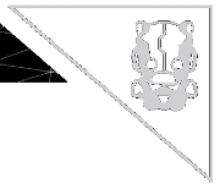
Appendix A: Overview of Risk Ratings and Finding Tables

Risk Ratings

To provide meaningful, quantitative analysis, IOActive uses an impact-versus-likelihood approach to scoring. For each finding, the assessment team assigns two ratings: one for impact and another for likelihood. Each rating corresponds to a numeric score ranging from 5 (critical) to 1 (informational). Table 2 explains each rating in terms of impact and likelihood.

Table 2. Rating and score as related to impact and likelihood

Rating (Score)	Impact	Likelihood
Critical (5)	Extreme impact to entire organization if exploited.	Vulnerability is almost certain to be exploited. Knowledge of the vulnerability and how to exploit it are in the public domain.
High (4)	Major impact to entire organization or single line of business if exploited.	Vulnerability is relatively easy to detect and exploit by an attacker with little skill.
Medium (3)	Noticeable impact to line of business if exploited.	A knowledgeable insider or expert attacker could exploit the vulnerability without much difficulty.
Low (2)	Minor damage if exploited or could be used in conjunction with other vulnerabilities to perform a more serious attack.	Exploiting the vulnerability would require considerable expertise and resources.
Informational (1)	Poor programming practice or poor design decision that may not represent an immediate risk on its own, but may have security implications if multiplied and/or combined with other vulnerabilities.	Vulnerability is not likely to be exploited on its own, but may be used to gain information for launching another attack.



IOActive calculates an aggregate risk score for each finding by multiplying its impact score by its likelihood score. For example, a finding with high likelihood and low impact would have an aggregate risk score of eight (8); that is, four (4) for high likelihood multiplied by two (2) for low impact. The aggregate risk score determines the finding's overall risk level, as shown in Table 3.

Table 3. Overall risk levels and corresponding aggregate scores

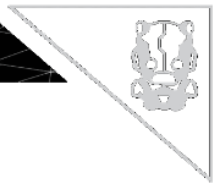
Overall Risk Level	Aggregate Risk Score (Impact multiplied by Likelihood)
Critical	20–25
High	12–19
Medium	6–11
Low	2–5
Informational	1

Finding Descriptors

IOActive's detailed findings tables provide a detailed description of what the consultants found, how those findings impact security, and what you should do to improve your security posture moving forward.

Threat and Impact. This field includes information about the vulnerability, including a specific and detailed description of the threat and what will happen if it is exploited. We include any applicable information for reproducing the finding, such as proof-of-concept code and the specific steps the consultants took to identify and exploit the finding. IOActive also provides screenshots, code blocks, static URLs, and any other relevant data that demonstrates the impact of the issue.

Recommendations. This field describes the actions required to prevent the vulnerability from being exploited. It may include specific step-by-step recommendations based on the assessment team's experience or more general recommendations based upon standard industry solutions.

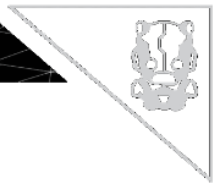


Finding Categories

IOActive categorizes findings using the vulnerability concepts described in Table 4.

Table 4. Vulnerability concepts

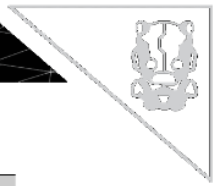
Concept	Description
Authentication	Confirming a user's identity or ensuring that a program can be trusted.
Access Controls	Methods used to authenticate the identity of a user, such as username and password combinations.
Broken Authentication and Session Management	Account credentials/session tokens are not protected properly, so attackers compromise passwords or keys to assume identities.
Configuration	How securely servers, devices, and software are chosen and implemented or deployed.
Cross-site Request Forgery	A browser is forced to send a pre-authenticated request to a vulnerable application, which then forces the browser to perform a hostile action that benefits the attacker.
Cross-site Scripting	When an application accepts user-supplied data and sends it to a web browser without first validating or encoding that content.
Cryptography and Insecure Storage	Applications rarely use mathematical data protections properly; attackers can conduct identity theft and credit card fraud.
Data Validation	Ensuring that a program operates on clean, correct, useful, and secure data.
Denial of Service	Anything that makes a computer resource unavailable to its intended users.
Failure to Restrict URL Access	When an application protects sensitive functionality by preventing its display as opposed to restricting access.
Information Leakage and Improper Error Handling	When an application exposes information about its configuration or internal function, or violates user privacy.
Insecure Communication	When an application fails to encrypt sensitive network traffic.
Insecure Direct Object Reference	When a reference to an internal implementation object (file, directory, database record, key, URL, etc.) is exposed.
Malicious File Execution	Code that is vulnerable to remote file inclusion allows attackers to include hostile code and data.
Session Management	The process of tracking a user's activity across sessions of interaction with a computer system.



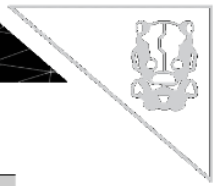
Appendix B: Scope

The consultants performed a detailed, line-by-line code review of the backend source codebase within the following key areas/folders:

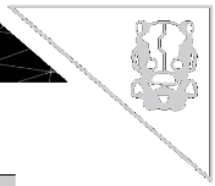
compound	pando
compound/handler	pando/handler
compound/handler/hc	pando/handler/hc
compound/handler/render	pando/handler/auth
compound/handler/param	pando/handler/render
compound/handler/codes	pando/handler/docs
compound/handler/views	pando/handler/param
compound/handler/rest	pando/handler/api
compound/cmd	pando/handler/api/user
compound/core	pando/handler/api/system
compound/core/proposal	pando/handler/api/actions
compound/config	pando/handler/request
compound/deploy	pando/handler/codes
compound/deploy/docker	pando/handler/node
compound/internal	pando/handler/node/oracle
compound/internal/compound	pando/handler/node/system
compound/internal/mixinet	pando/handler/rpc
compound/docs	pando/handler/rpc/api
compound/docs/images	pando/handler/rpc/views
compound/builds	pando/handler/acl
compound/service	pando/cmd
compound/service/operation	pando/cmd/pando-cli
compound/service/message	pando/cmd/pando-cli/internal
compound/service/supply	pando/cmd/pando-cli/internal/column
compound/service/proposal	pando/cmd/pando-cli/internal/cfg
compound/service/borrow	pando/cmd/pando-cli/internal/call



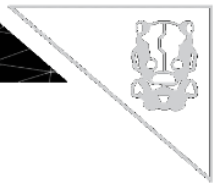
compound	pando
compound/service/wallet	pando/cmd/pando-cli/internal/jq
compound/service/market	pando/cmd/pando-cli/cmds
compound/service/account	pando/cmd/pando-cli/cmds/cat
compound/service/block	pando/cmd/pando-cli/cmds/config
compound/worker	pando/cmd/pando-cli/cmds/auth
compound/worker/cashier	pando/cmd/pando-cli/cmds/oracle
compound/worker/snapshot	pando/cmd/pando-cli/cmds/pay
compound/worker/message	pando/cmd/pando-cli/cmds/flip
compound/worker/spentsync	pando/cmd/pando-cli/cmds/vat
compound/worker/txsender	pando/cmd/pando-cli/cmds/tx
compound/worker/syncer	pando/cmd/pando-cli/cmds/use
compound/pkg	pando/cmd/pando-cli/cmds/sys
compound/pkg/resthttp	pando/cmd/pando-cli/cmds/proposal
compound/pkg/mtg	pando/cmd/pando-cli/cmds/actions
compound/pkg/number	pando/cmd/pando-server
compound/pkg/concurrency	pando/cmd/pando-server/config
compound/pkg/id	pando/cmd/pando-worker
compound/pkg/aes	pando/cmd/pando-worker/config
compound/store	pando/docker
compound/store/operation	pando/core
compound/store/transaction	pando/notifier
compound/store/oracle	pando/mock
compound/store/message	pando/internal
compound/store/user	pando/internal/request
compound/store/supply	pando/server
compound/store/proposal	pando/parliament
compound/store/borrow	pando/parliament/testdata
compound/store/wallet	pando/parliament/files



compound	pando
compound/store/market	pando/service
	pando/service/asset
mixin-sdk-go	pando/service/oracle
mixin-sdk-go/edwards25519	pando/service/oracle/dirtoracle
mixin-sdk-go/logo	pando/service/message
mixin-sdk-go/_examples	pando/service/user
mixin-sdk-go/_examples/oauth_ed25519	pando/service/wallet
mixin-sdk-go/_examples/blaze	pando/worker
mixin-sdk-go/_examples/oauth	pando/worker/pricesync
mixin-sdk-go/_examples/echo_api	pando/worker/cashier
mixin-sdk-go/_examples/multisig	pando/worker/spentsync
mixin-sdk-go/_examples/mixinnet	pando/worker/messenger
mixin-sdk-go/_examples/nodemonitor	pando/worker/txsender
mixin-sdk-go/_examples/wallet	pando/worker/datadog
mixin-sdk-go/_examples/echo_proxy	pando/worker/keeper
	pando/worker/keeper/wallet
	pando/worker/syncer
	pando/worker/events
	pando/worker/payee
	pando/worker/payee/wallet
	pando/worker/assigner
	pando/metric
	pando/assets
	pando/assets/i18n
	pando/pkg
	pando/pkg/mtg
	pando/pkg/mtg/types
	pando/pkg/number



compound	pando
	pando/pkg/maker
	pando/pkg/maker/cat
	pando/pkg/maker/makertest
	pando/pkg/maker/oracle
	pando/pkg/maker/flip
	pando/pkg/maker/vat
	pando/pkg/maker/sys
	pando/pkg/maker/proposal
	pando/pkg/uuid
	pando/pkg/reversetwirp
	pando/pkg/aes
	pando/store
	pando/store/transaction
	pando/store/asset
	pando/store/oracle
	pando/store/flip
	pando/store/message
	pando/store/user
	pando/store/proposal
	pando/store/collateral
	pando/store/wallet
	pando/store/dbtest
	pando/store/vault
	pando/store/vault/testdata
	pando/session



The team used the cloc[1] tool to get a complete breakdown of the lines based on programming language. The results are as follows:

Compound

```
github.com/AlDanial/cloc v 1.90  T=0.10 s (1372.5 files/s, 113925.7 lines/s)
-------------------------------------------------------------------------------
Language                     files          blank        comment           code
-------------------------------------------------------------------------------
Go                             124           1758            538           8022
Markdown                         5            185              0            474
YAML                             2              8              0             74
make                             1              8              1             26
Dockerfile                       1             10              4             12
Bourne Shell                     1              1              0              2
-------------------------------------------------------------------------------
SUM:                           134           1970            543           8610
-------------------------------------------------------------------------------
```

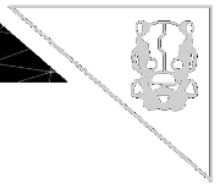
Mixin-SDK

```
github.com/AlDanial/cloc v 1.90  T=0.08 s (1043.6 files/s, 133762.9 lines/s)
-------------------------------------------------------------------------------
Language                     files          blank        comment           code
-------------------------------------------------------------------------------
Go                              76           1341            269           8538
Markdown                         4             34              0             72
-------------------------------------------------------------------------------
SUM:                            80           1375            269           8610
-------------------------------------------------------------------------------
```

Pando

```
github.com/AlDanial/cloc v 1.90  T=0.18 s (1536.8 files/s, 170055.9 lines/s)
-------------------------------------------------------------------------------
Language                     files          blank        comment           code
-------------------------------------------------------------------------------
Go                             243           3734            956          21430
JSON                             2              0              0           1141
YAML                             9             57             19           1041
Markdown                         8            294              0            715
XML                              7              0              0            370
Protocol Buffers                 1             37             35            223
Dockerfile                       2             20              0             26
-------------------------------------------------------------------------------
SUM:                           272           4142           1010          24946
-------------------------------------------------------------------------------
```

[1] github.com/AlDanial/cloc



Total Lines

```
github.com/AlDanial/cloc v 1.90  T=0.30 s (1586.4 files/s, 169160.0 lines/s)
-------------------------------------------------------------------------------
Language                     files          blank        comment           code
-------------------------------------------------------------------------------
Go                             436           6745           1754          37687
Markdown                        17            513              0           1261
JSON                             2              0              0           1141
YAML                            11             65             19           1115
XML                              7              0              0            370
Protocol Buffers                 1             37             35            223
Dockerfile                       3             30              4             38
make                             1              8              1             26
Bourne Shell                     1              1              0              2
-------------------------------------------------------------------------------
SUM:                           479           7399           1813          41863
```