IOActive Security Advisory

Title	Confide Messaging Application – Multiple Critical Vulnerabilities
Severity	Critical
Discovered by	Mike Davis, Ryan O’Horo, Nick Achatz
Advisory Date	March 8, 2017

Affected Products

Confide messaging application, published by Confide, Inc. (https://getconfide.com/)

Impact

A malicious attacker could potentially perform one or more of the following behaviors:

- Impersonate another user by hijacking their account session
- Impersonate another user by guessing their password
- Learn the contact details of all or specific Confide users
- Become an intermediary in a conversation and decrypt messages
- Alter the contents of a message or attachment in transit without first decrypting it

Background

The Confide application is marketed as a “confidential messenger,” incorporating several features, including “military grade end-to-end encryption,” designed to protect the secrecy of sent messages.

Confide’s first known availability was as an iOS application in February of 2014.

Technical Details

IOActive uncovered numerous security issues at the time of testing:

- HTTPS
  - The application’s notification system did not require a valid SSL server certificate to communicate, which would leak session information to actors performing a man-in-the-middle attack.
- Messaging
  - Unencrypted messages could be transmitted, and the user interface made no indication when unencrypted messages were received.
  - The application uploaded file attachments before the user sends the intended message.

  - The application failed to use authenticated encryption, allowing Confide to alter messages in-transit.
  - Confide failed to provide a participant fingerprint authentication mechanism, allowing Confide to conduct man-in-the-middle attacks on encrypted messages by changing the public keys sent to parties of a conversation.
  - Attackers could send malformed messages which crash, slow, or otherwise disrupt the application.
- Account Management
  - The application allowed an attacker to enumerate all Confide user accounts, including real names, e-mail addresses, and phone numbers.
  - The application failed to prevent brute-force attacks on user account passwords.
  - Users were permitted to choose short, easy-to-guess passwords.
- Website
  - The application's website was vulnerable to an arbitrary URL redirection, which could facilitate social engineering attacks against its users.
  - The application's website reflected incorrectly entered passwords back to the browser.

Testing versions 4.0.4 for Android and 1.4.2 for Windows and OS X, IOActive was able to recover over 7,000 records for users registered between the dates of 2017-02-22 to 2017-02-24. This data also indicated that between 800,000 and one million user records were potentially contained in the database.

In the following anonymized example records, IOActive found that the returned data's structure implied that the full database row was being returned, effectively including any user data Confide possesses for that user.

The data provided by the Confide API is described as follows:

- Username: Randomly generated eight-character string used internally
- Verified: `True` if the user has clicked the provided verification link
- UserId: A predictably incremented record identifier
- PublicKey: The user's public key(s)
- Phone: The user's phone number(s)
- Email: The user's email address(es)

Sample record 1:

```
{
'Username': u'xyzdwmvx',
'Verified': True,
'FirstName': u'Ricky',
'LastName': u'Ricardo',
'SignupDate': u'2017-02-24T21:01:18Z',
'UserId': 123228,
'PublicKey':
[u'0344238CABCDEFGHIJBE7F5AB54B4DCD861FEAEB28369B73F5EC1B54D9C299
4972']
'Email': [u'ricardo@domain.gov']
}
```

Sample record 2:

```
{
'Username': u'xyzd22bc',
'Verified': True,
'FirstName': u'Jae',
'Phone': [u'+15555555555'],
'LastName': u'Day',
'SignupDate': u'2017-02-24T15:48:10Z',
'UserId': 123506,
'PublicKey':
[u'0370CC40ABCDEFGHIJ24448F243BE4EC7947743D7070F81FF0DB884AEA7C0C
0070'],
'Email': [u'jday@domain.com']
}
```

Fixes

After IOActive disclosed these vulnerabilities to Confide, the company subsequently remediated issues identified as critical and informed IOActive of fixes.

Timeline

February 2017: IOActive conducts testing on the Confide application.

February 25, 2017: Confide begins fixing issues uncovered by the detection of anomalous behavior during the testing window.

February 27, 2017: IOActive contacts Confide via several public email addresses to establish a line of communication.

February 28, 2017: IOActive discloses issues to Confide. Confide communicates that some mitigations are already in progress and plans are being made to address all issues.

March 2, 2017: Confide releases an updated Windows client (1.4.3), which includes fixes that address some of IOActive's findings.

March 3, 2017:	Confide informs IOActive that remediation of critical issues is complete.
March 8, 2017:	Findings are published.