Issued 3/10/17

Secure' Messaging App Riddled with Security Flaws

A messaging app reportedly popular with White House aides had several security issues that could have resulted in user details being exposed, security researchers have announced.

According to researchers at IOActive, Confide, an encrypted messaging service for Windows, Android and Apple devices, had “multiple security vulnerabilities of varying severities.”
The main issues discovered by IOActive’s researchers included the application’s notification system not requiring a valid SSL server certificate to communicate. This meant sessions were vulnerable to man-in-the-middle (MITM) attacks.

Messages did not have to be encrypted when sent, and users were given no indication when an unencrypted message was sent, IOActive said. The app also failed to use authenticated encryption, meaning messages could have been altered in transit. Also on the messaging front, there was no participant fingerprint authentication mechanism. This could have resulted in MITM attacks.

In terms of account management, users were allowed to pick short, easy-to-use passwords, and the application did nothing to stop brute-force attacks. This is where an attacker tries multiple different passwords to gain

access to the account - given there was no enforcement of strong passwords, brute-force attackers were likely to be successful pretty quickly. Another serious flaw in the account management on Confide meant researchers were able to establish details of all Confide users, including names, phone numbers and email addresses.

The vulnerabilities could have resulted in a hacker gaining access to the app, where they could have impersonated another user by hijacking their account session or by guessing their password. Additionally, flaws could have exposed contact details to the hacker. If reports that the app is popular among President Donald Trump's aides at the White House are true, the potential data leakage could have been disastrous.

The attacker could also have become an intermediary in a conversation and decrypt messages, and alter the contents of a message or attachment in transit without first decrypting it, IOActive said.

In their tests researchers were able to see details relating to 7000 users and found evidence that between 800,000 and one million users were contained in the database. The issue here was that Confide's API appeared to be returning the full database row, essentially exposing all the data Confide held on a user.

Confide has seen huge growth in its user base since the start of 2017, after reports emerged that many people at the White House were using it to communicate securely and anonymously both with each other and members of the media. Confide claims to use "military-grade end-to-end encryption" and messages self destruct after being read.

IOActive shared all its findings with Confide, who said the issues have now been fixed. "This is a great example of how responsible disclosure between

researchers and vendors can work when both sides are engaged in making security a focus," said Jennifer Steffens, CEO of IOActive.
"When our researchers connected with Confide to disclose the vulnerabilities they were receptive to our research, quick to move on addressing critical issues found, and worked with us to share the information. From 18 years of experience in security research, we know just how rare this interaction is, yet collaborative information exchange and responsiveness are the baseline for successful responsible disclosures. We wish more firms were as responsive and committed to quick resolution of identified issues," Steffens added.