xx network security advisory [30 July 2022]

Last Updated: 30 Jul 2022 5:17PM EST

Systems Affected

- Messages sent by iOS and Android xx messenger up to and including version 4.1.0 may be affected when quantum computers are available that can break 3072-bit DH Key exchanges.

Overview

Early today, July 30th 2022, a paper [1] was released which describes how to recover keys in the SIDH key exchange that is used by the xx messenger. While xx messenger does not use the key encapsulation mechanism described in the paper [2], known as SIKE [3], the xx messenger team has concluded that the SIDH side of the key exchange for xx messenger is vulnerable to the techniques in the paper.

The xx messenger is secure as the messenger uses a hybrid system where traditional DH key exchange is combined with the SIDH key exchange to establish end-to-end authenticated channels. However, once an attacker is able to break the DH key exchange algorithm, i.e. with a quantum computer of sufficient power, messages sent with xx messenger under the current key exchange (versions <= 4.1.0) may be vulnerable to compromise by an attacker.

Description

Supersingular isogeny Diffie–Hellman key exchange (SIDH) was a post-quantum cryptographic algorithm for key agreement. SIDH boasted one of the smallest key sizes of all post-quantum key exchanges and supported perfect forward secrecy, making it a good candidate to replace existing cryptographic key exchange mechanisms. A version of SIDH had advanced to the fourth round of NIST's Post-Quantum Cryptography standardization process in July of 2022 [4].

The paper [1] recovers the secret key from data sent publicly as part of the key exchange protocol, and specifically attacks the SIKE [3] protocol. It uses a feature of the starting elliptic curve with the torsion point information on the secret part of the curve sent publicly during the key exchange to recover the secret key. The paper was

able to show secret key recovery in SIKEp434 parameters, as well as SIKEp503, SIKEp610 and SIKEp751.

The xx messenger uses a hybrid system (see the source code in [2]). A 3072-bit DH key agreement is separately established from a SIDH key agreement using SIKEp503 parameters. The results of each operation are subsequently hashed together to form the final key. While the SIDH part of the key agreement is vulnerable to the paper [1], the DH part is not. Therefore, the xx messenger is not presently vulnerable to this attack but messages sent using versions up to and including 4.1.0 may be vulnerable at some point in the future if an attacker has collected and stored them for future analysis.

An attacker would need to take key exchange messages from cMix, break the 3072-bit DH encryption, then break the SIKEp503 SIDH key using the attack. Because the cMix network does not store message long term, an attacker must collect these key exchange messages in one of 2 ways:

1. Passively record all traffic from the last node in a cMix round to the other nodes, then break the 4096 bit RSA-based TLS keys on this traffic to reveal the cMix messages.
2. Find the target's reception identity, track the network with that identity for messages, and actively download any that come in for the target.

The xx team congratulates and thanks the authors, Wouter Castryck and Thomas Decru, for finding this attack and publishing it. Work like this is critical to ensuring the cryptography we use is safe and secure.

Impact

In practice, this flaw may allow a global adversary recording all traffic in the network or conducting targeted surveillance against a known reception ID to decrypt that user's traffic after the advent of quantum computers that can break 3072-bit DH key exchanges.

Solution

The xx messenger team is accelerating pre-existing plans to switch to CSIDH [5] after we confirm it is not vulnerable to this attack. The next version of xx messenger, version 4.2.0, will replace the SIDH key exchange and should be released in a few weeks. The CSIDH key exchange does not contain auxiliary torsion point information relied on by the attack, and it should be generally immune to this type of attack.

References

1. "An efficient key recovery attack on SIDH (preliminary version)" by *Wouter Castryck*, KU Leuven and *Thomas Decru*, KU Leuven - https://eprint.iacr.org/2022/975
2. DH and SIDH hybrid key exchange in xx messenger source code - https://git.xx.network/elixxir/client/-/blob/3937cfb100d96304725b64a46eed1e69914633c5/e2e/ratchet/partner/session/cypher.go#L25
3. https://sike.org/
4. "PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates" - US NIST - https://csrc.nist.gov/news/2022/pqc-candidates-to-be-standardized-and-round-4
5. "CSIDH: An efficient post-quantum commutative group action" by Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. - https://csidh.isogeny.org/index.html