From: Joost Rijneveld <joost@joostrijneveld.nl>
Sent: Tuesday, March 13, 2018 10:03 AM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: SPHINCS+

Dear all,

It was brought to our attention that the SPHINCS+ reference code contains an error that causes a longer-than-necessary message digest to be generated and signed (contradicting the specification). We have fixed the code and updated it on our web page. Note that, as this also affects the leaf index selection, the fix causes incompatibility with the previous version of the code.

Thanks go to Dorian Amiet for spotting the bug and alerting us to it.

Cheers,
Joost Rijneveld, on behalf of the SPHINCS+ team

From: Thomas Prest <thomas.prest@ens.fr>
Sent: Friday, April 13, 2018 4:28 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: SPHINCS+

Dear all,

This mail is to inform you of a fault injection attack against SPHINCS+ and Gravity-SPHINCS.
In schemes of the SPHINCS family, the signing algorithm essentially consists of reconstructing a bunch of Merkle trees and signing their roots with one-time signatures (OTS).
Introducing one single random fault during the reconstruction of the penultimate Merkle tree has the effect that one OTS signs two different values, which can then be exploited to forge signatures for any message for a computational cost of computing about 2^34 hashes.

More detailed information can be found here:
- Article:
https://eprint.iacr.org/2018/102
- Slides: https://tprest.github.io/Slides/grafting-trees-pqcrypto.pdf
We have informed the submitters about this attack, and to the best of our knowledge they agree with the claims made in our article.

We want to emphasize that this is a fault injection attack: it does not question the security of these schemes when the signing algorithm is executed normally.

Best,
Laurent, Ange and Thomas