Cryptology ePrint Archive

Paper 2023/331

A Vulnerability in Implementations of SHA-3, SHAKE, EdDSA, and Other NIST-Approved Algorithms

Nicky Mouha, Strativia, Largo, MD, USA
Christopher Celi, National Institute of Standards and Technology, Gaithersburg, MD, USA

Abstract

This paper describes a vulnerability in several implementations of the Secure Hash Algorithm 3 (SHA-3) that have been released by its designers. The vulnerability has been present since the final-round update of Keccak was submitted to the National Institute of Standards and Technology (NIST) SHA-3 hash function competition in January 2011, and is present in the eXtended Keccak Code Package (XKCP) of the Keccak team. It affects all software projects that have integrated this code, such as the scripting languages Python and PHP Hypertext Preprocessor (PHP). The vulnerability is a buffer overflow that allows attacker-controlled values to be eXclusive-ORed (XORed) into memory (without any restrictions on values to be XORed and even far beyond the location of the original buffer), thereby making many standard protection measures against buffer overflows (e.g., canary values) completely ineffective. First, we provide Python and PHP scripts that cause segmentation faults when vulnerable versions of the interpreters are used. Then, we show how this vulnerability can be used to construct second preimages and preimages for the implementation, and we provide a specially constructed file that, when hashed, allows the attacker to execute arbitrary code on the victim's device. The vulnerability applies to all hash value sizes, and all 64-bit

introduce the Init-Update-Final Test (IUFT) to detect this vulnerability in implementations.

Metadata

Available format(s)

PDF

Category

Implementation

Publication info

Published elsewhere. CT-RSA 2023

DOI

10.1007/978-3-031-30872-7_1

Keywords

CVE-2022-37454 SHA-3 Keccak hash function vulnerability

Contact author(s)

nicky @ mouha be
christopher celi @ nist gov

History

2023-04-28: revised

2023-03-06: received

See all versions

Short URL

https://ia.cr/2023/331

Cryptology ePrint Archive

BibTeX Copy to clipboard

```
@misc{cryptoeprint:2023/331,
      author = {Nicky Mouha and Christopher Celi},
      title = {A Vulnerability in Implementations of {SHA}-3,
      howpublished = {Cryptology {ePrint} Archive, Paper 202
      year = {2023},
      doi = {10.1007/978-3-031-30872-7_1},
      url = {https://eprint.iacr.org/2023/331}
}
```