RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

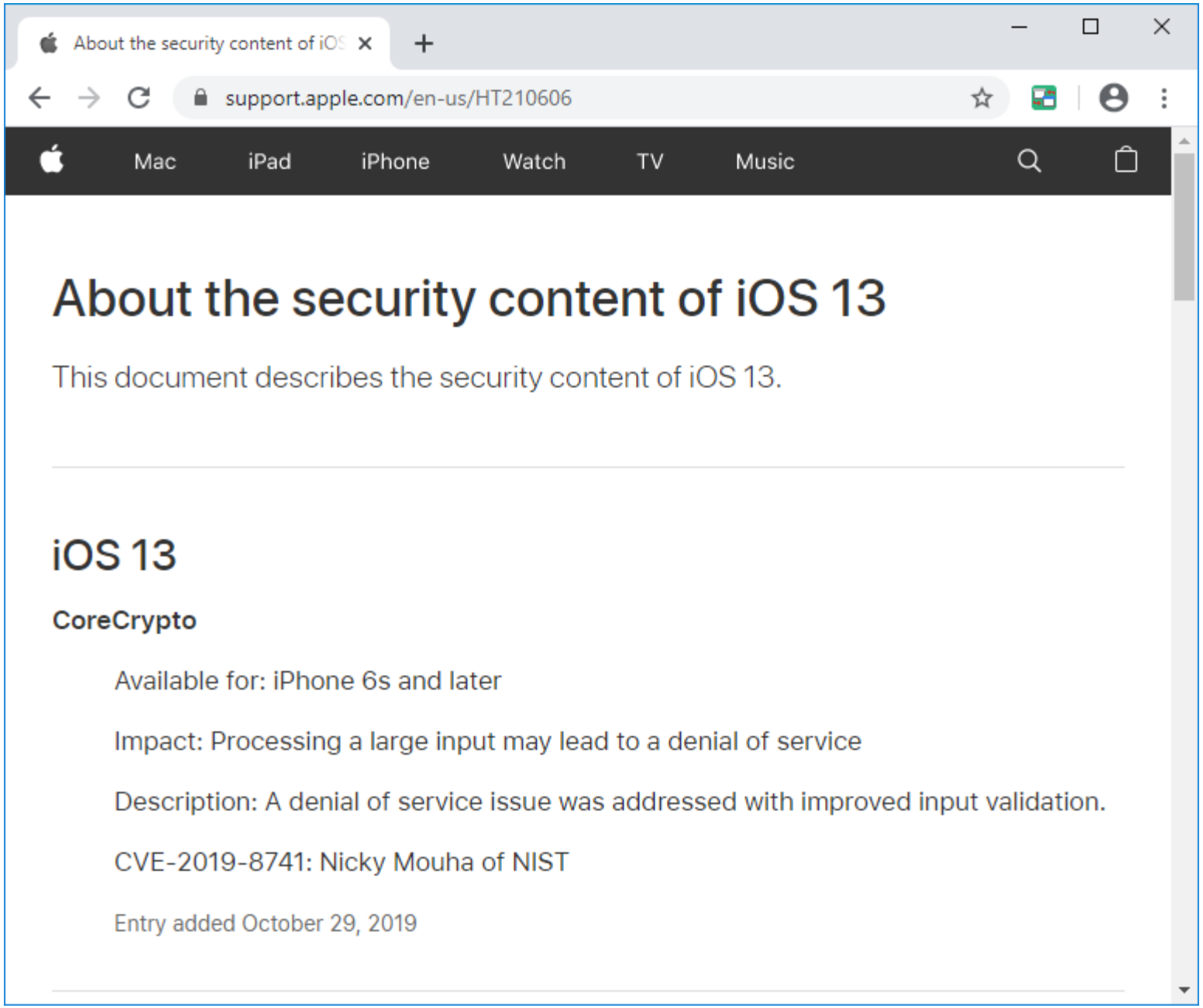
HUMAN ELEMENT

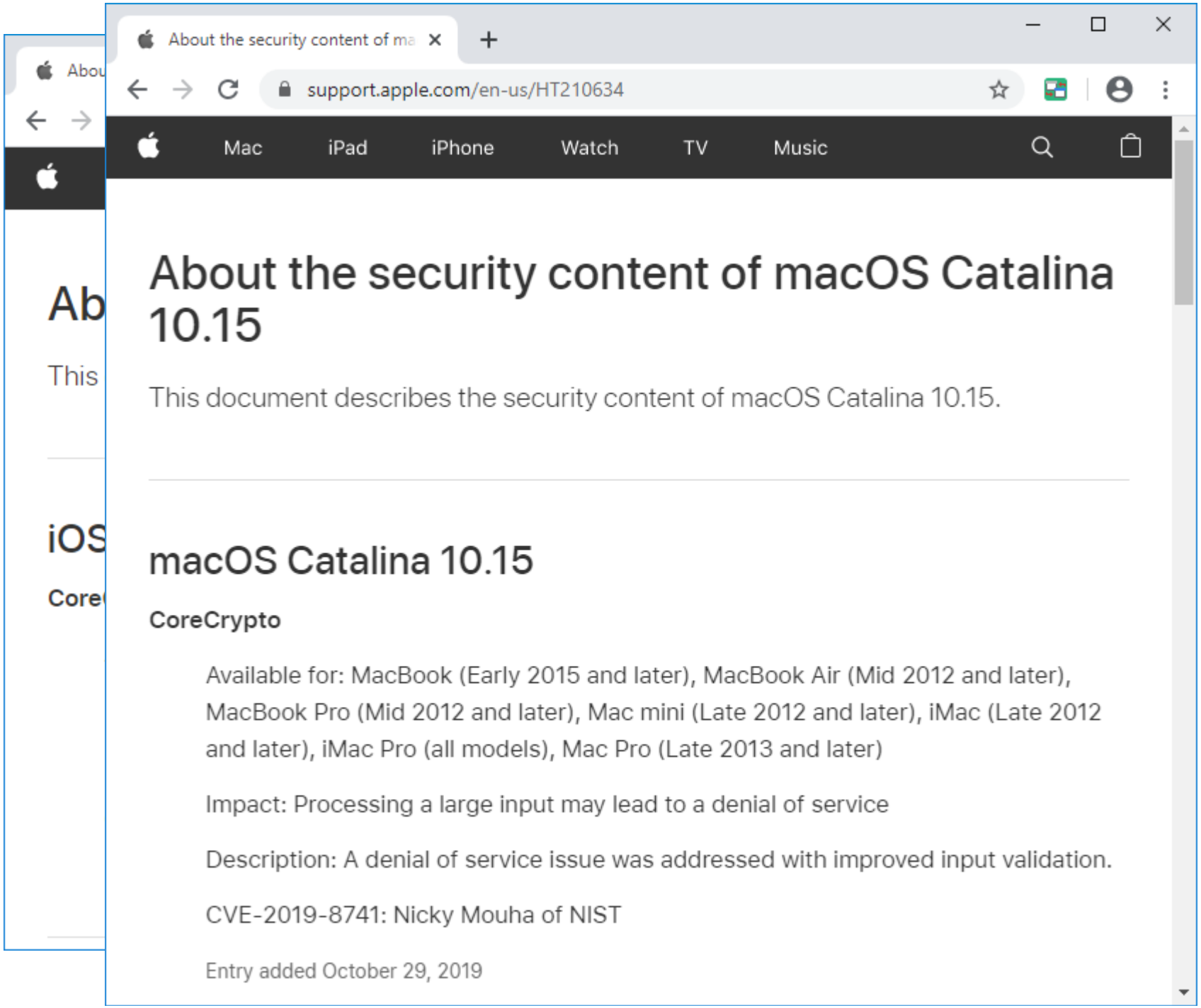
SESSION ID: CRYP-T12

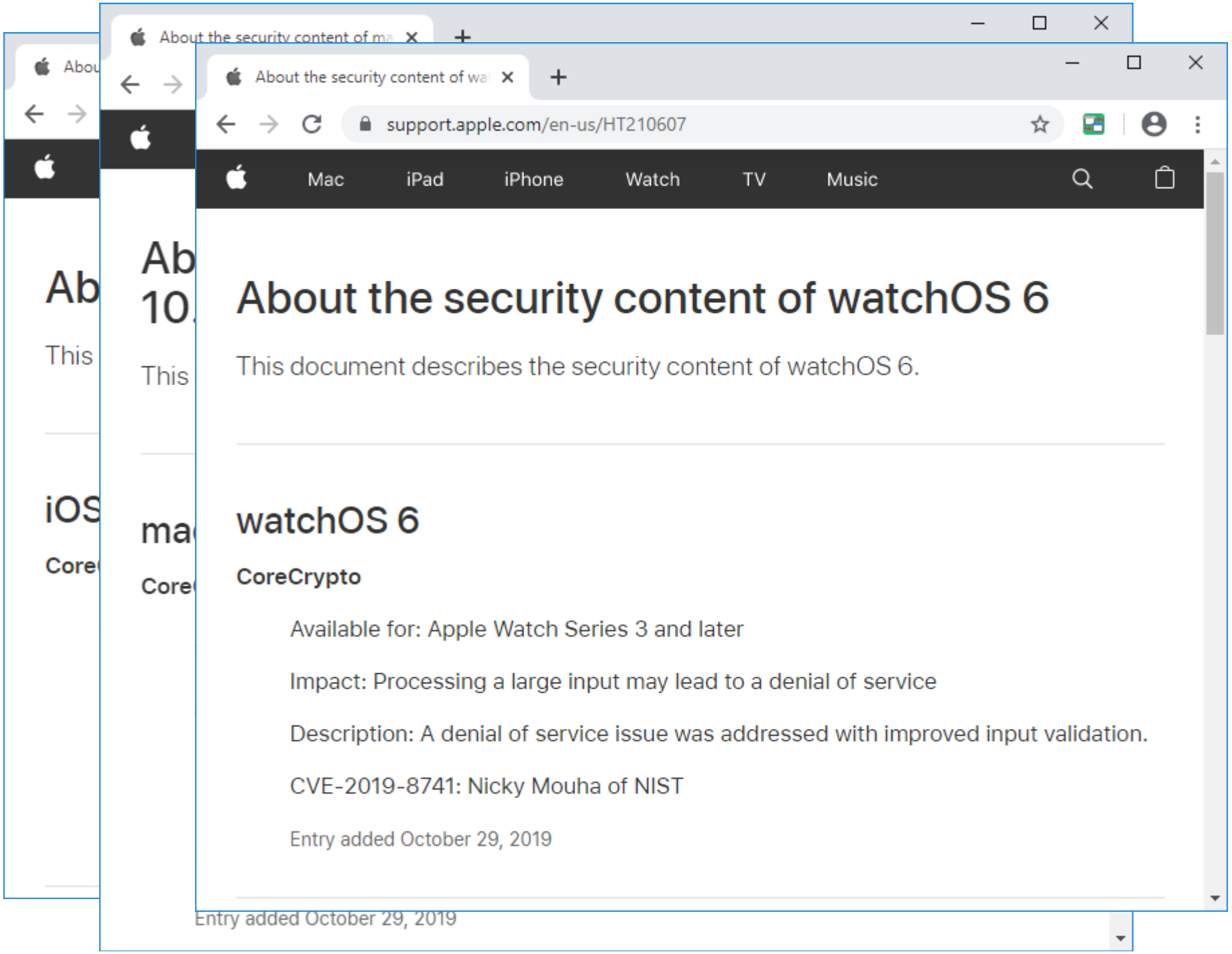
Extending NIST's CAVP Testing of Cryptographic Hash Function Implementations

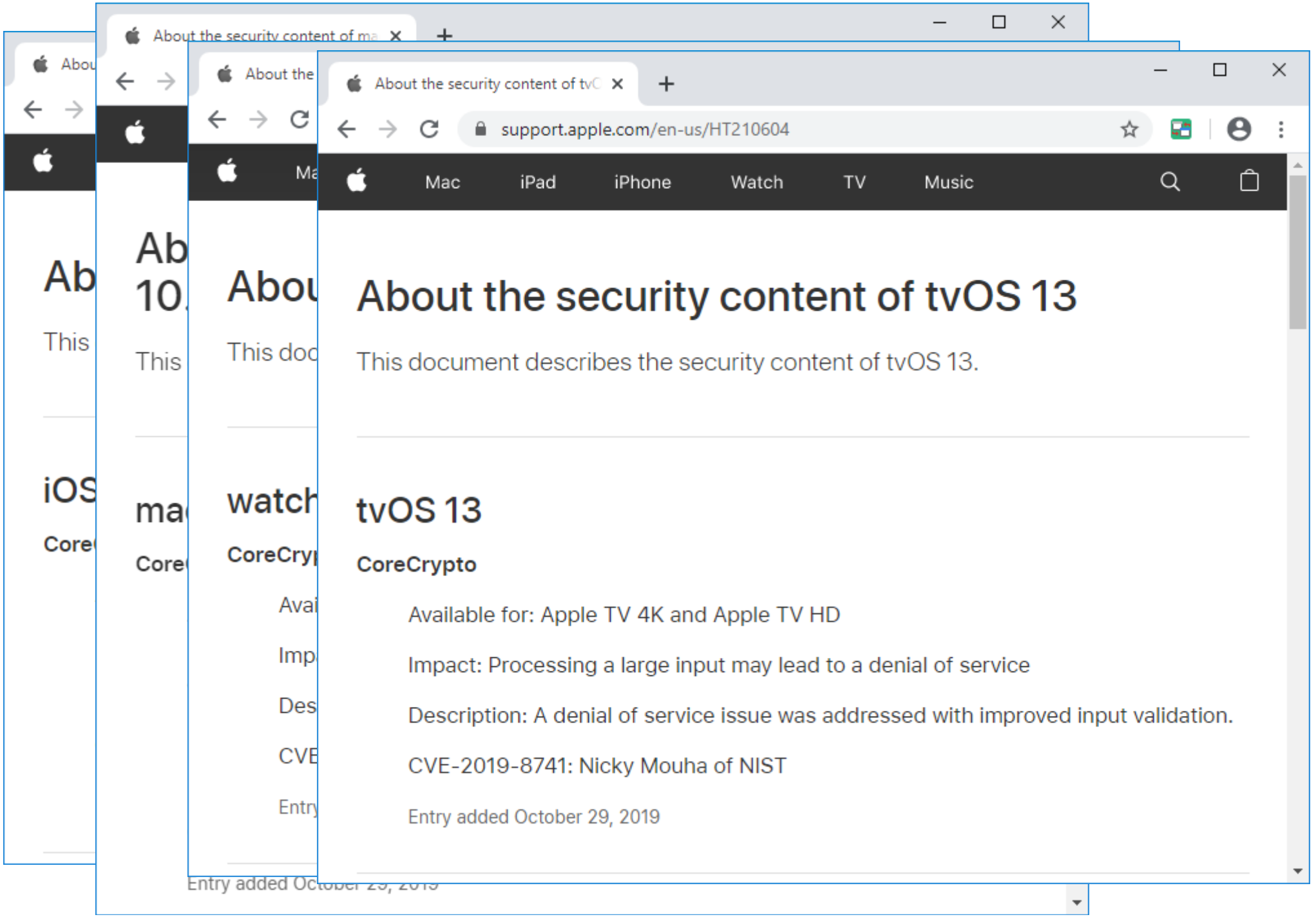
Nicky Mouha and Christopher Celi

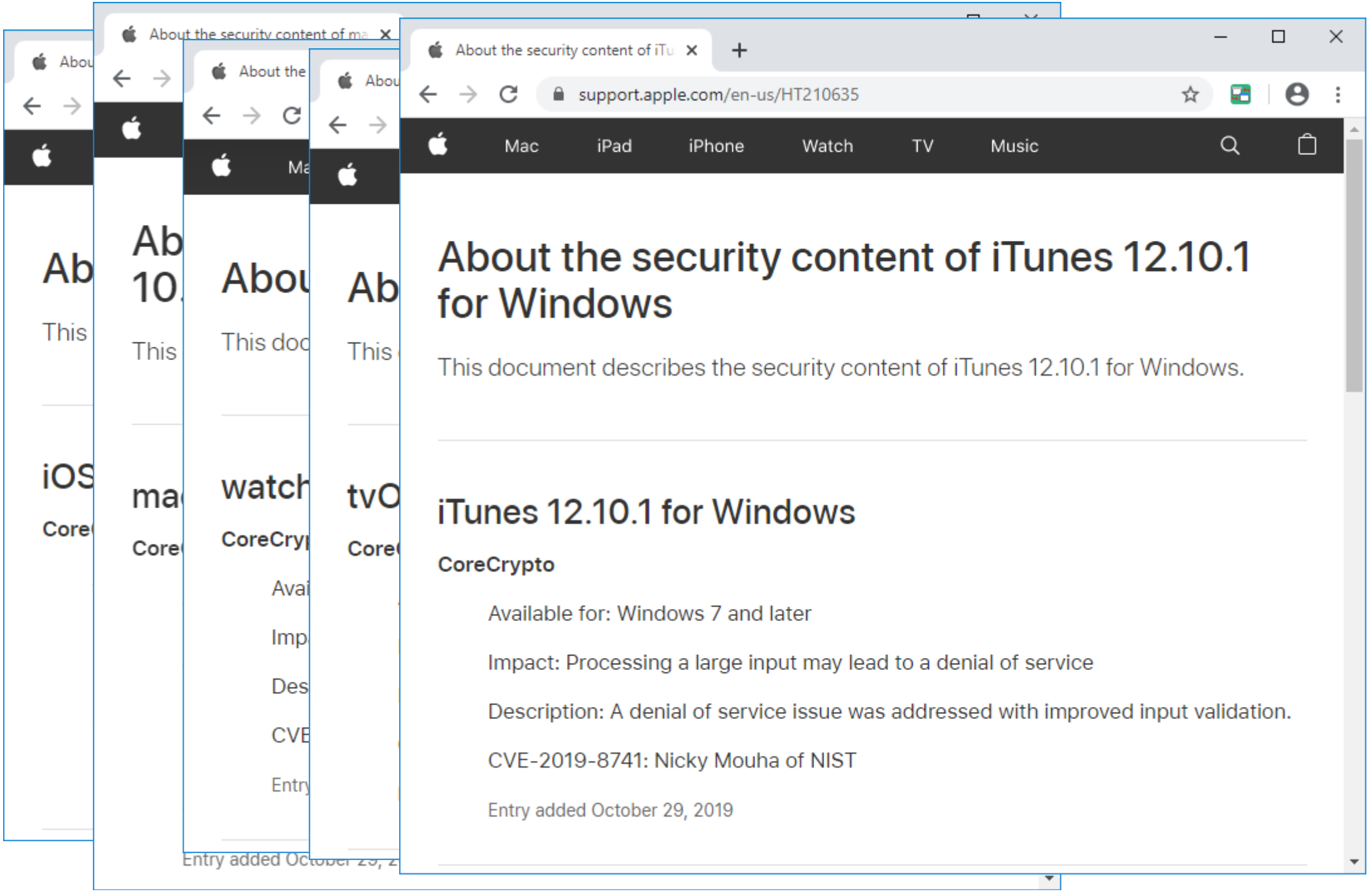
National Institute of Standards and Technology (NIST)

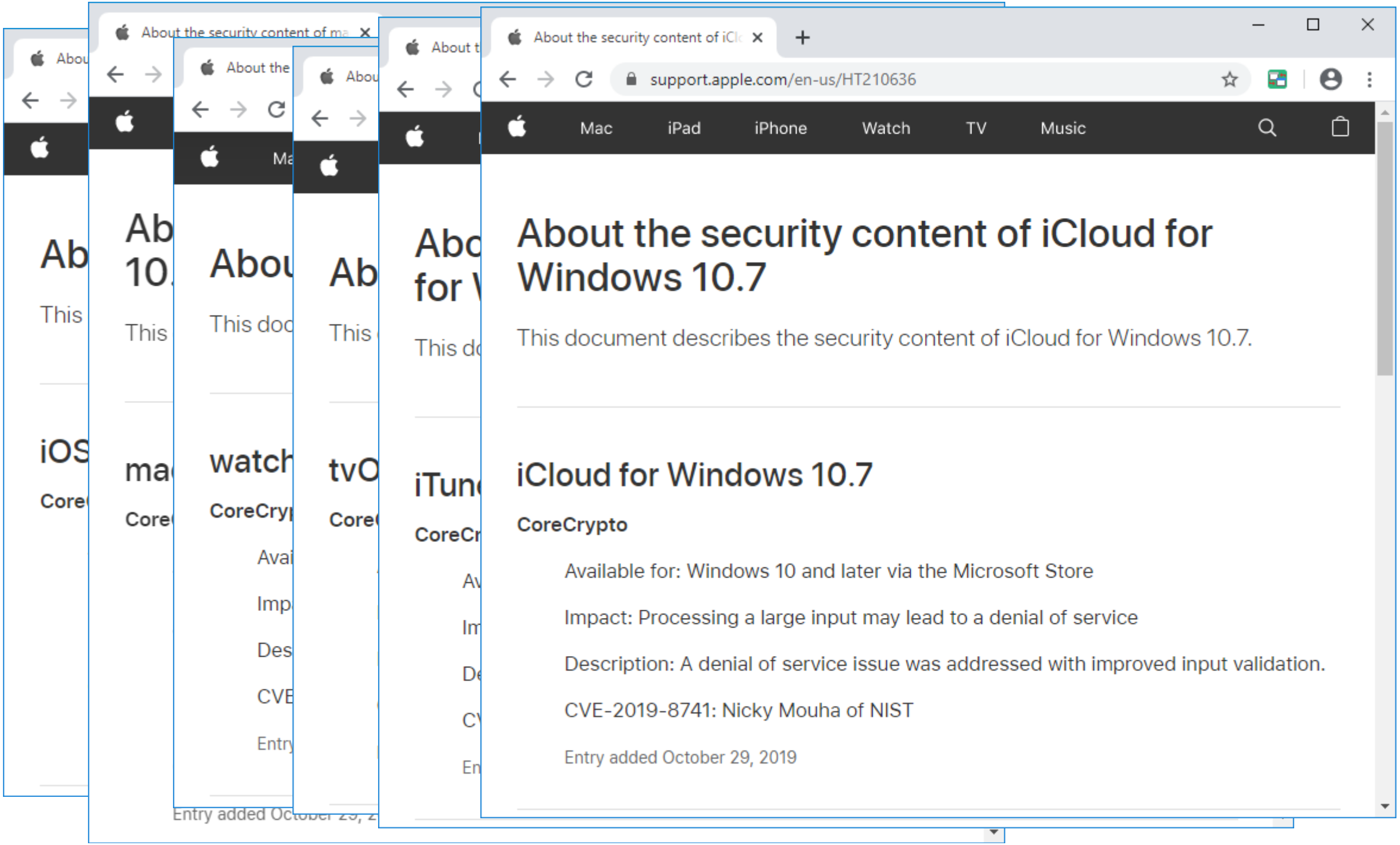

About the security content of iOS
support.apple.com/en-us/HT210606
Mac
iPad
iPhone
Watch
TV
Music
About the security content of iOS 13
This document describes the security content of iOS 13.
iOS 13
CoreCrypto
Available for: iPhone 6s and later
Impact: Processing a large input may lead to a denial of service
Description: A denial of service issue was addressed with improved input validation.
CVE-2019-8741: Nicky Mouha of NIST
Entry added October 29, 2019

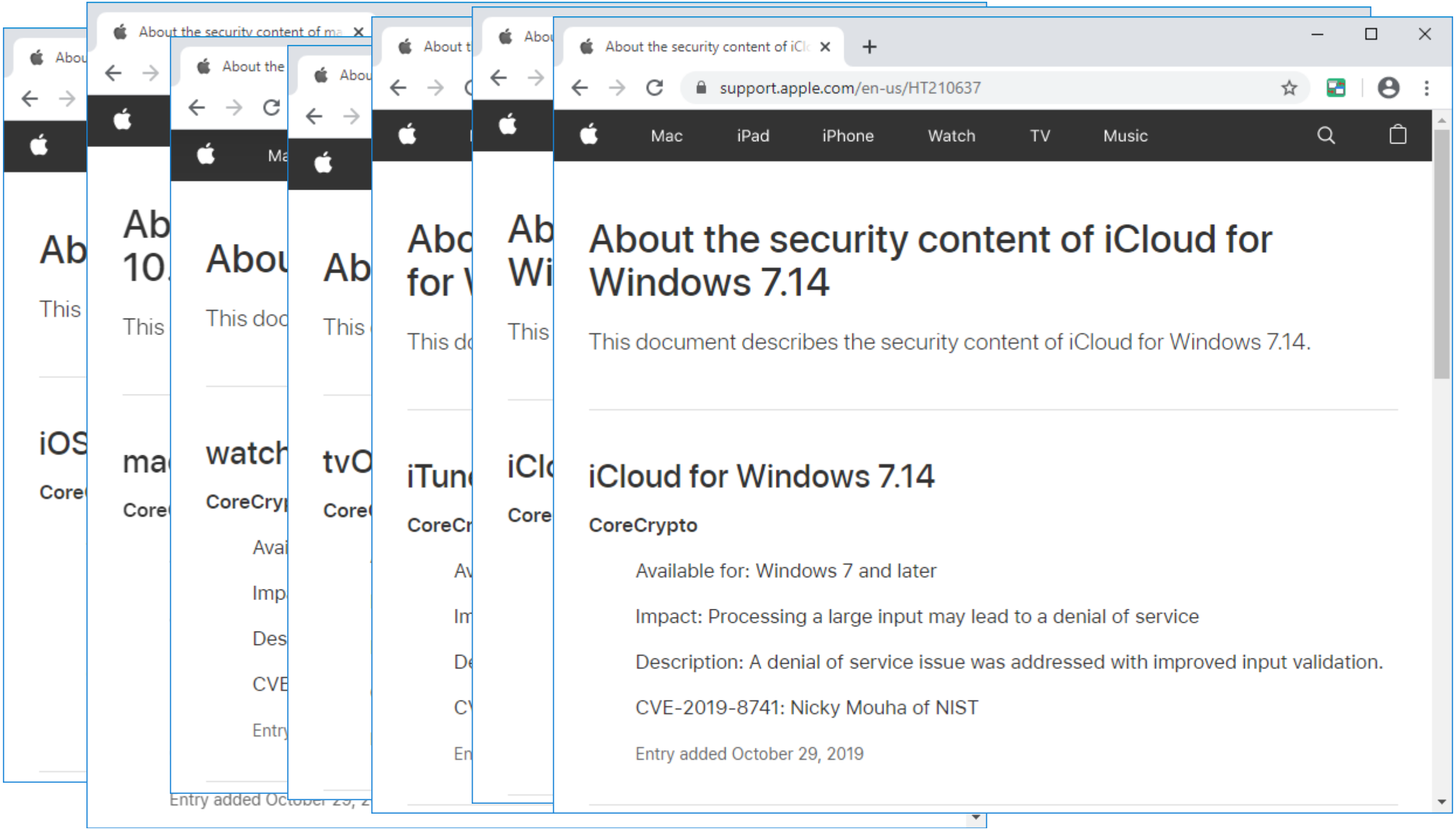

About the security content of ma
support.apple.com/en-us/HT210634
Mac
iPad
iPhone
Watch
TV
Music
About the security content of macOS Catalina 10.15
This document describes the security content of macOS Catalina 10.15.
macOS Catalina 10.15
CoreCrypto
Available for: MacBook (Early 2015 and later), MacBook Air (Mid 2012 and later), MacBook Pro (Mid 2012 and later), Mac mini (Late 2012 and later), iMac (Late 2012 and later), iMac Pro (all models), Mac Pro (Late 2013 and later)
Impact: Processing a large input may lead to a denial of service
Description: A denial of service issue was addressed with improved input validation.
CVE-2019-8741: Nicky Mouha of NIST
Entry added October 29, 2019


About the security content of watchOS 6
support.apple.com/en-us/HT210607
Mac
iPad
iPhone
Watch
TV
Music
About the security content of watchOS 6
This document describes the security content of watchOS 6.
watchOS 6
CoreCrypto
Available for: Apple Watch Series 3 and later
Impact: Processing a large input may lead to a denial of service
Description: A denial of service issue was addressed with improved input validation.
CVE-2019-8741: Nicky Mouha of NIST
Entry added October 29, 2019


About the security content of tvC
support.apple.com/en-us/HT210604
Mac
iPad
iPhone
Watch
TV
Music
About the security content of tvOS 13
This document describes the security content of tvOS 13.
tvOS 13
CoreCrypto
Available for: Apple TV 4K and Apple TV HD
Impact: Processing a large input may lead to a denial of service
Description: A denial of service issue was addressed with improved input validation.
CVE-2019-8741: Nicky Mouha of NIST
Entry added October 29, 2019


About the security content of iTu
support.apple.com/en-us/HT210635
Mac
iPad
iPhone
Watch
TV
Music
About the security content of iTunes 12.10.1 for Windows
This document describes the security content of iTunes 12.10.1 for Windows.
iTunes 12.10.1 for Windows
CoreCrypto
Available for: Windows 7 and later
Impact: Processing a large input may lead to a denial of service
Description: A denial of service issue was addressed with improved input validation.
CVE-2019-8741: Nicky Mouha of NIST
Entry added October 29, 2019


About the security content of iCloud for Windows 10.7
support.apple.com/en-us/HT210636
Mac
iPad
iPhone
Watch
TV
Music
About the security content of iCloud for Windows 10.7
This document describes the security content of iCloud for Windows 10.7.
iCloud for Windows 10.7
CoreCrypto
Available for: Windows 10 and later via the Microsoft Store
Impact: Processing a large input may lead to a denial of service
Description: A denial of service issue was addressed with improved input validation.
CVE-2019-8741: Nicky Mouha of NIST
Entry added October 29, 2019


About the security content of iCloud for Windows 7.14
support.apple.com/en-us/HT210637
Mac
iPad
iPhone
Watch
TV
Music
About the security content of iCloud for Windows 7.14
This document describes the security content of iCloud for Windows 7.14.
iCloud for Windows 7.14
CoreCrypto
Available for: Windows 7 and later
Impact: Processing a large input may lead to a denial of service
Description: A denial of service issue was addressed with improved input validation.
CVE-2019-8741: Nicky Mouha of NIST
Entry added October 29, 2019


CRYPTANALYSIS

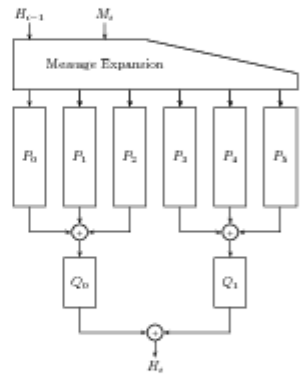
RSAConference2020

A Little Bit of History…

The LANE hash function

What is LANE?

LANE is a cryptographic hash function that has been entered as a candidate in the NIST SHA-3 competition by the COSIC research group of the Katholieke Universiteit Leuven, Belgium. The aims of LANE are to be secure, easy to understand, elegant and flexible in implementation. It reuses components from the AES block cipher. LANE can take advantage of the parallelism offered by modern high-performance CPUs, but also scales down to embedded systems. Another advantages of LANE is the fact that its design is supported by a clear design rationale and a comprehensive security analysis.



The LANE compression function

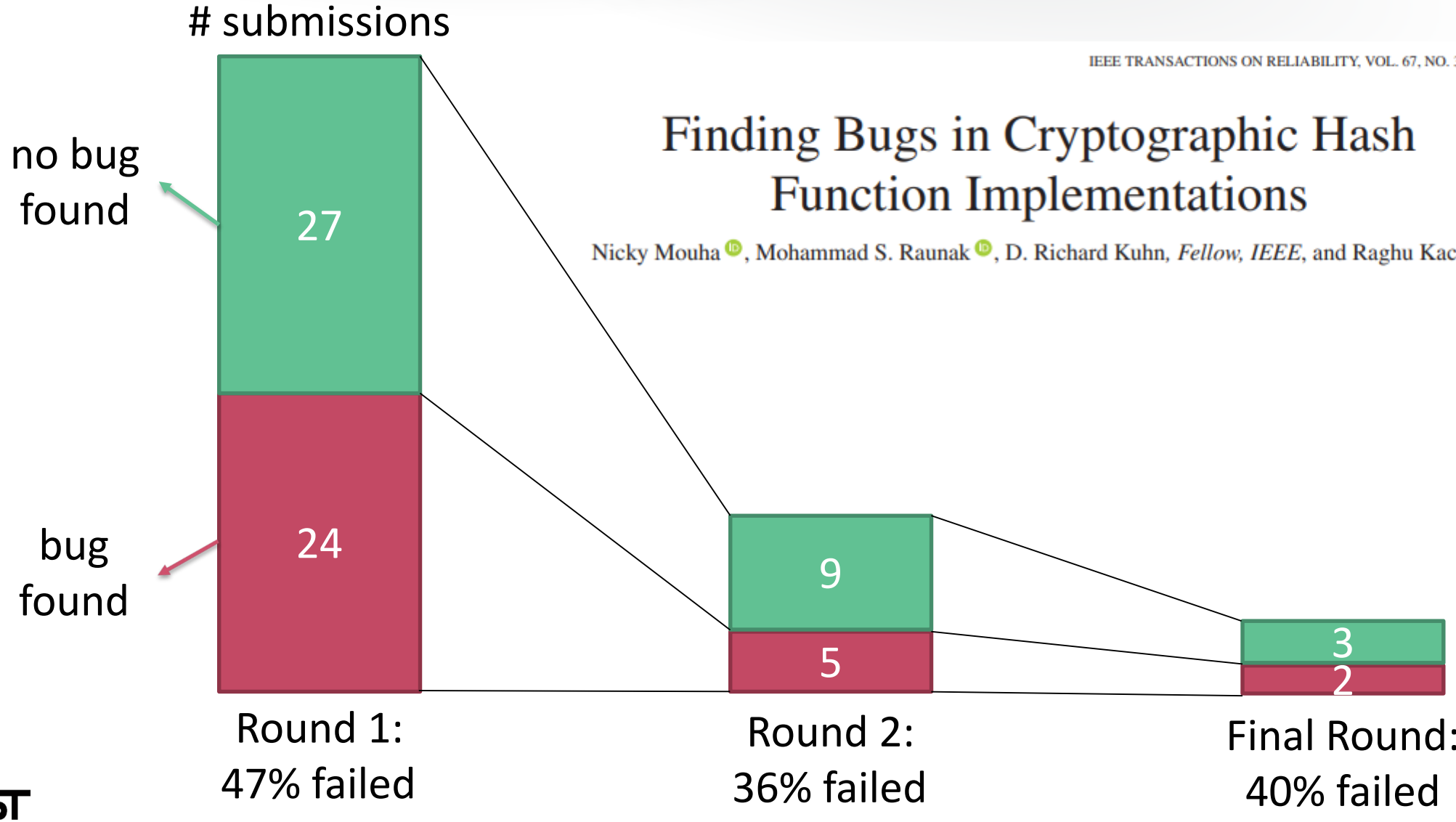
LANE was designed by Sebastiaan Indesteege. Important contributions to the design and the security analysis were made by Elena Andreeva, Christophe De Cannière, Orr Dunkelman, Emilia Käsper, Svetla Nikova, Bart Preneel and Elmar Tischhauser, all from the COSIC research group of the Katholieke Universiteit Leuven, Belgium.

More information on LANE is available here.

The SHA-3 competition

The American National Institute of Standards and Technology (NIST) has initiated a public competition, the SHA-3 competition, to develop a new cryptographic hash algorithm. This is an algorithm that maps a message of variable length into a short, fixed-length digest, such that certain security properties, like collision resistance and preimage resistance, are achieved.

SHA-3 Competition Bugs

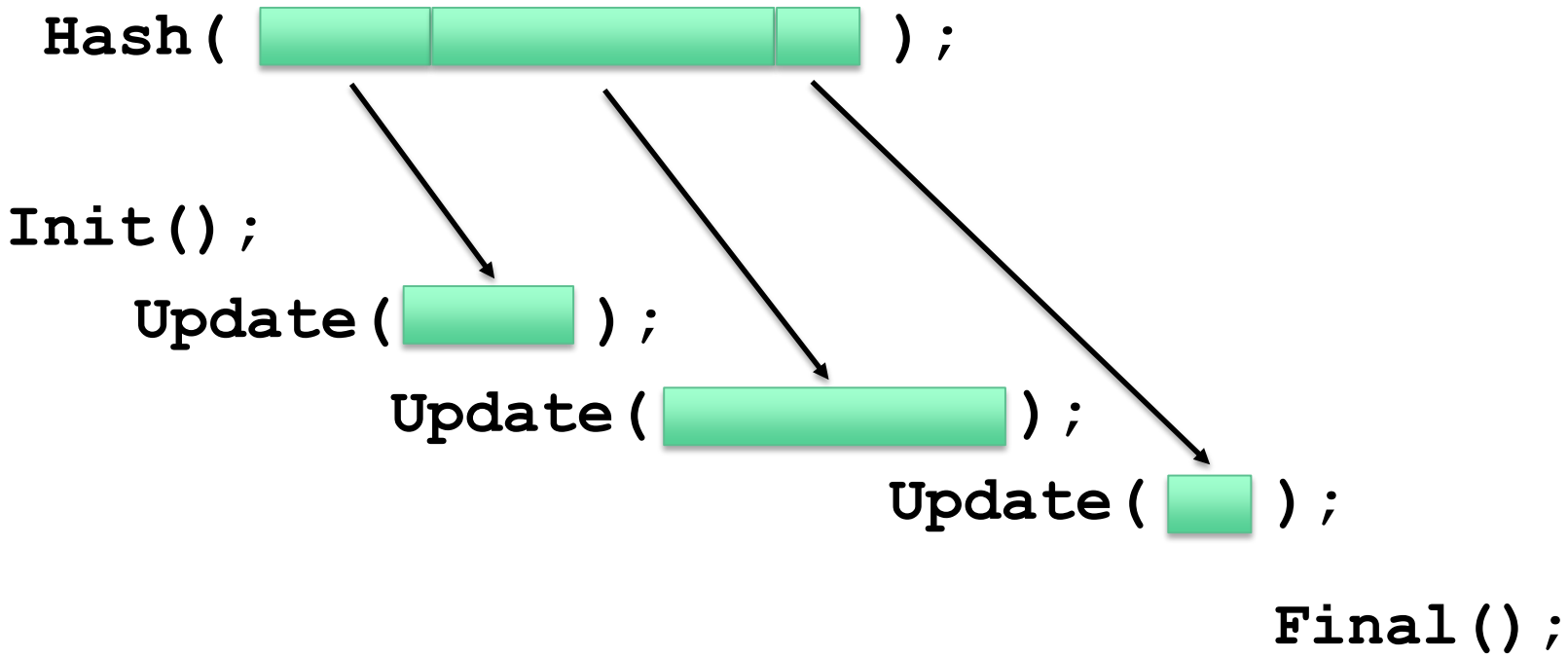


IEEE TRANSACTIONS ON RELIABILITY, VOL. 67, NO. 3, SEPTEMBER 2018

Finding Bugs in Cryptographic Hash Function Implementations

Nicky Mouha, Mohammad S. Raunak, D. Richard Kuhn, *Fellow, IEEE*, and Raghu Kacker

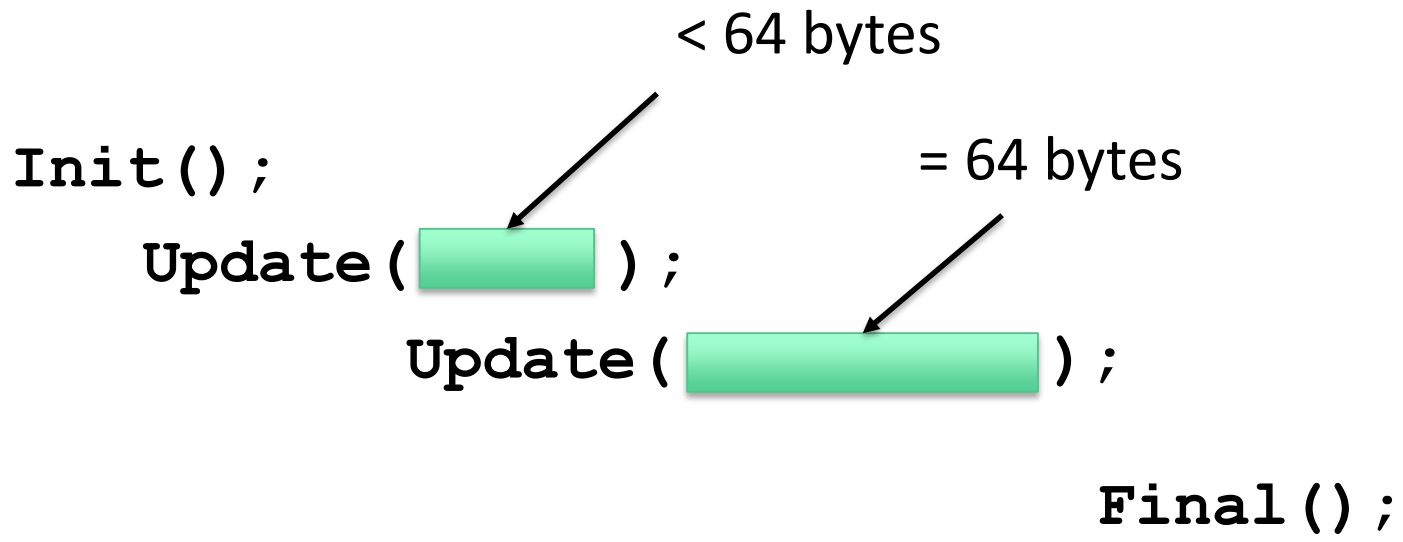
Two Common Hash Function Interfaces



Q: Where/when are they used?

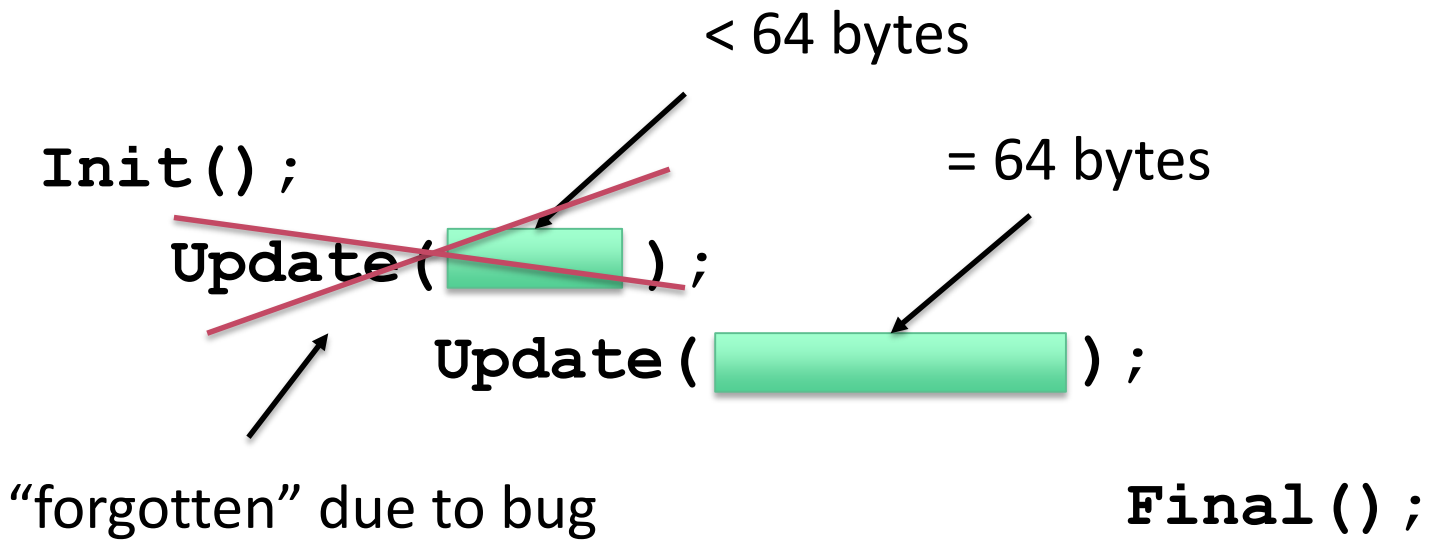
BLAKE Bug

BLAKE-256: processes message in blocks of 64 bytes



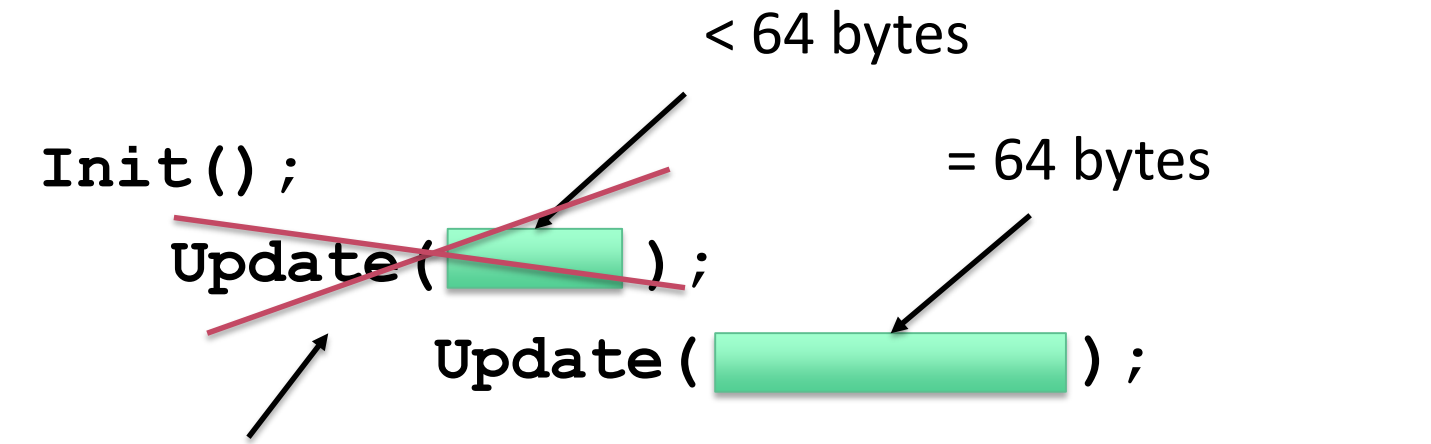
BLAKE Bug

BLAKE-256: processes message in blocks of 64 bytes



BLAKE Bug

BLAKE-256: processes message in blocks of 64 bytes



"second preimage"
(modified message, same hash)

RSAConference2020

Real-World Impact?

Apple CoreCrypto: Hash Functions

- CoreCrypto
  - Cryptographic module in all Apple devices
- Vulnerability
  - Incorrect handling of long ($\geq$ 4 GiB) messages
  - Affects 11/12 hash functions
  - Infinite loop

Algorithm	Block size (in bytes)	Vulnerable
MD2	16	✗
MD4	64	✓
MD5	64	✓
RIPEMD-128	64	✓
RIPEMD-160	64	✓
RIPEMD-256	64	✓
RIPEMD-320	64	✓
SHA-1	64	✓
SHA-224	64	✓
SHA-256	64	✓
SHA-384	128	✓
SHA-512	128	✓

Apple CoreCrypto: Vulnerable Code

Lines 75-87 of **`ccdigest_update()`** in **`ccdigest/src/ccdigest_update.c`**:

```
// low-end processors are slow on division
if (di->block_size == 1<<6) { // sha256
  nblocks = len >> 6;
  nbytes = len & 0xFFFFffC0;
} else if (di->block_size == 1<<7) { // sha512
  nblocks = len >> 7;
  nbytes = len & 0xFFFFff80;
} else {
  nblocks = len / di->block_size;
  nbytes = nblocks * di->block_size;
}
```

Apple CoreCrypto: Updated (January 2020)

Lines 27-36 of **`ccdigest_update()`** in **`ccdigest/src/ccdigest_update.c`**:

```
if (di->block_size == 1<<6) { // md5 & sha1 & sha256
  nblocks = len >> 6;
  nbytes = nblocks << 6;
} else if (di->block_size == 1<<7) { // sha384 & sha512
  nblocks = len >> 7;
  nbytes = nblocks << 7;
} else {
  nblocks = len / di->block_size;
  nbytes = nblocks * di->block_size;
}
```

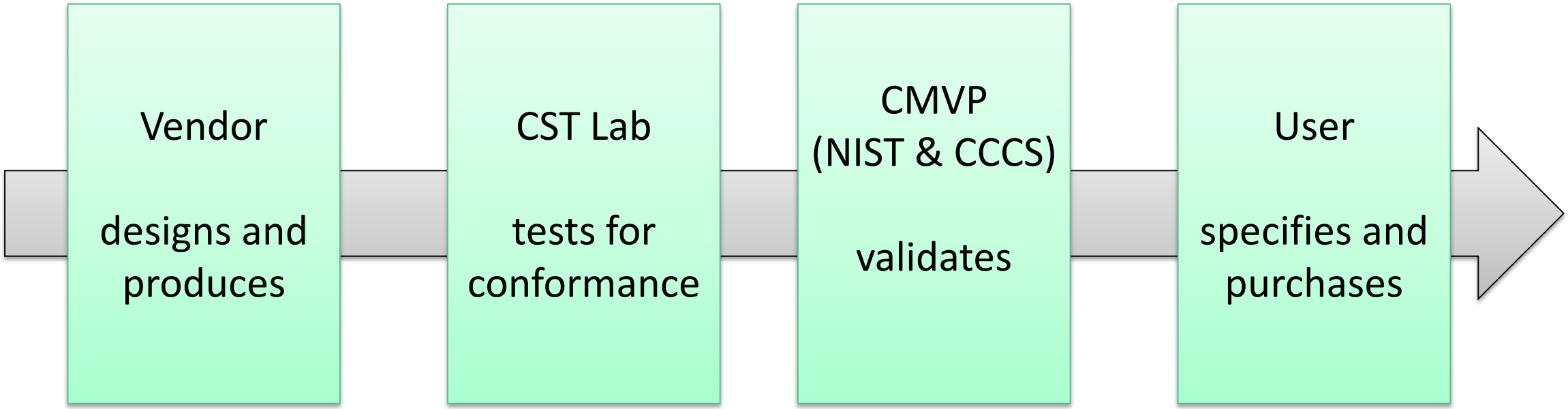
Apple CoreCrypto: Other Vulnerable Algorithms

- HMAC
- Ed25519
- SRP
  - strlen() on null-terminated string
- ~~ANSI X9.63 KDF~~
  - Not vulnerable due to range check
  - Source code comment: “ccdigest_update only supports 32-bit length”
- …?

RSAConference2020

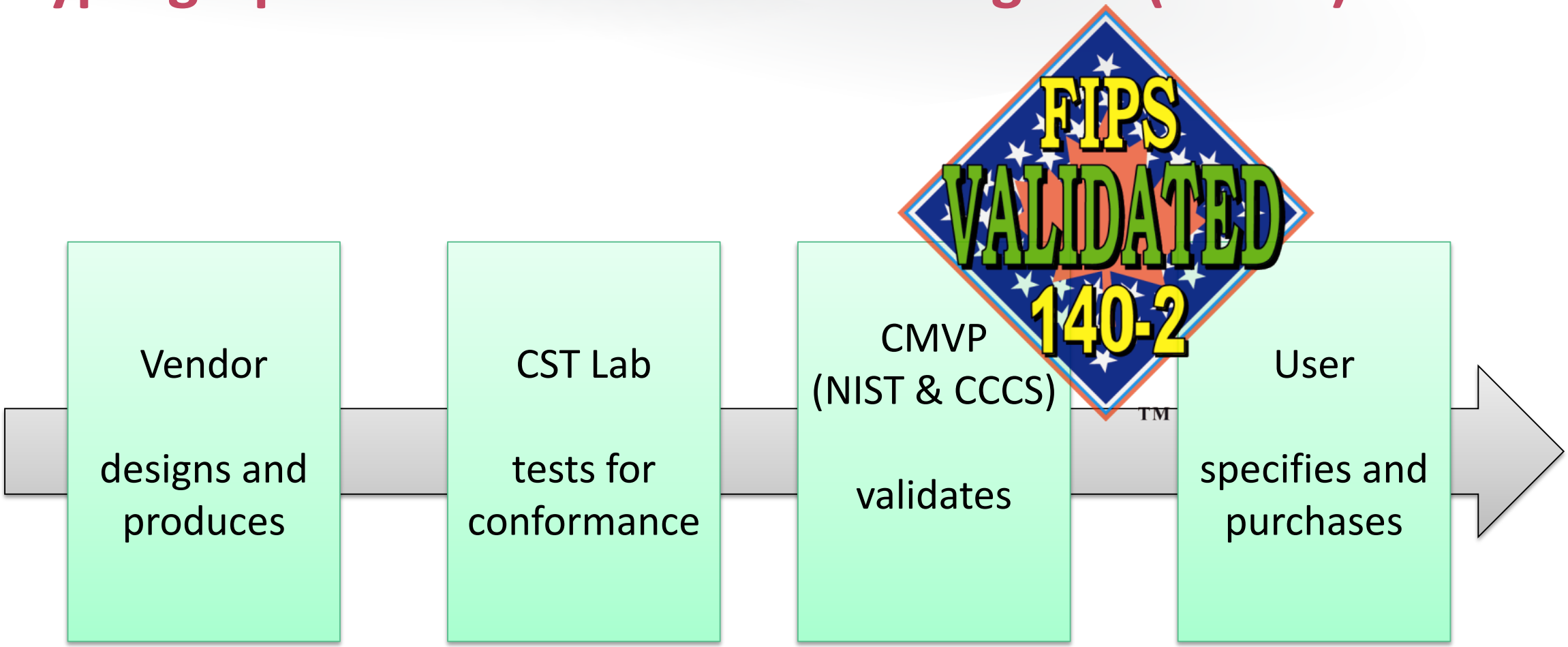
NIST to the Rescue…

Cryptographic Module Validation Program (CMVP)



CAVP: prerequisite for CMVP
ACVP: protocol used by CAVP

Cryptographic Module Validation Program (CMVP)



CAVP: prerequisite for CMVP
ACVP: protocol used by CAVP

ACVP JSON Format

Algorithm Functional Test (AFT) request:

```
{
  "msg": "BCE7",
  "len": 16
}
```

AFT response (for SHA-224):

```
{
  "md": "1FA29E9B23060562F9370453EF817E18C56AE844E5B85F2ED34B4B38"
}
```

NIST SHAVS Document

- *"While the specification for SHA specifies that messages up to at least $2^{64} - 1$ bits are possible, these tests only test messages up to a limited size of approximately 100,000 bits. This is adequate for detecting algorithmic and implementation errors."*

  — The Secure Hash Algorithm Validation System (SHAVS), NIST

Large Data Test (LDT)

LDT request:

```
{
  "largeMsg": {
    "content": "D6F7",
    "contentLength": 16,
    "fullLength": 34359738368,
    "expansionTechnique": "repeating" }
}
```

LDT response (for SHA-224):

```
{
  "md": "BA94D02FBE63F0B858AFABF3F98AAED1CD9DE45A2D1120D661214EF1"
}
```

Apply What You Have Learned Today

- CVE: not end, but beginning
  - Usually: patch and forget
  - Better: avoid systematically
- Discuss bugs in cryptography
  - Dive into your own experience
  - Talk to your colleagues
- Reach out to us!