Exploit Detail and Vulnerability Causes:

Sha-1 has a very apparent weakness where it allows flexible message length as the input and outputs a tag representing its internal state. Knowing this, an attacker can build a message with a correct tag without ever having to know what the secret key is. The tag for any given message is simply the concatenated H vectors after running the sha-1 algorithm

Attack Reliability:

The implemented attack is extremely reliable and can work for any randomly generated 64-bit key.

Run-time Complexity:

The general exploit run time complexity would take roughly twice the time to pad a message and twice the time to run the Sha-1 algorithm. The specific run time for my exploit on a variety of machines was:

Machine	Run Time
Macbook Air 2013	Real 0m19.989s user 0m0.100ssys0m0.155s
Macbook Pro 2016	0.05s user 0.02s system 88% cpu 0.077 total
Macbook Pro 2017	0.05s user 0.02s system 88% cpu 0.082 total

Vulnerability Solutions:

One way to solve the Sha-1 exploit would be to prohibit allowing message blocks to chain together in order to get a valid tag. Another thing on top of this can be to encrypt the final output using the same key and Sha-1 or even another IND-CPA secure encryption scheme. If this were the case, an attacker would be prevented from knowing the initial state of the Sha-1 scheme after running the first message.