Weak Cryptographic Hash: Missing Required Step Mitigation SOP

# Development Mitigation SOP

The generation of cryptographic hashes involves multiple steps, and missing any required step compromises the strength of the generated hashes.

# Defense Against [DEFECT]

Brief explanation of how to mitigate defect

# Examples

## General Example

…

MessageDigest messageDigest = MessageDigest.getInstance(“SHA-512”);

io.writeLine(MyUtilClass.bytesToHex(messageDigest.digest()));

…

## Explanation

An explanation of why the above code is vulnerable

## Recommendation

The code below… explanation of why the following code is fixed

…

String data = “This is a message to be digested using MD5”;

MessageDigest messageDigest;

try {

messageDigest = MessageDigest.getInstance(“MD5”);

messageDigest.updatte(data.getBytes());

…

**Resources**

1. [Fortify Taxonomy: Software Security Errors](https://vulncat.hpefod.com/en/detail?id=desc.controlflow.java.weak_cryptographic_hash_missing_required_step" \l "Java%2FJSP)