# CVE Detail – CVE-2019-10071

The code which checks HMAC in form submissions used String.equals() for comparisons, which results in a timing side channel for the comparison of the HMAC signatures. This could lead to remote code execution if an attacker is able to determine the correct signature for their payload. The comparison should be done with a constant time algorithm instead.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.92611

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-203: Observable Discrepancy

## CAPEC(s)

* CAPEC-189: Black Box Reverse Engineering

## Affected Products

* cpe:2.3:a:apache:tapestry:\*:\*:\*:\*:\*:\*:\*:\*