# CWE Detail – CWE-1236

## Description

The product saves user-provided information into a Comma-Separated Value (CSV) file, but it does not neutralize or incorrectly neutralizes special elements that could be interpreted as a command when the file is opened by a spreadsheet product.

## Extended Description

User-provided data is often saved to traditional databases. This data can be exported to a CSV file, which allows users to read the data using spreadsheet software such as Excel, Numbers, or Calc. This software interprets entries beginning with '=' as formulas, which are then executed by the spreadsheet software. The software's formula language often allows methods to access hyperlinks or the local command line, and frequently allows enough characters to invoke an entire script. Attackers can populate data fields which, when saved to a CSV file, may attempt information exfiltration or other malicious activity when automatically executed by the spreadsheet software.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2019-12134: Low privileged user can trigger CSV injection through a contact form field value

**•** CVE-2019-4521: Cloud management product allows arbitrary command execution via CSV injection

**•** CVE-2019-17661: CSV injection in content management system via formula code in a first or last name

## Modes of Introduction

**•** Implementation: The weakness is in the implementation of a software's CSV export feature, in particular how it formats formula entries as the output gets flattened into a text file.

## Common Consequences

**•** Impact: Read Application Data, Execute Unauthorized Code or Commands — Notes: Current versions of Excel warn users of untrusted content.

## Potential Mitigations

**•** Implementation: When generating CSV output, ensure that formula-sensitive metacharacters are effectively escaped or removed from all data before storage in the resultant CSV. Risky characters include '=' (equal), '+' (plus), '-' (minus), and '@' (at). (Effectiveness: Moderate)

**•** Implementation: If a field starts with a formula character, prepend it with a ' (single apostrophe), which prevents Excel from executing the formula. (Effectiveness: Moderate)

**•** Architecture and Design: Certain implementations of spreadsheet software might disallow formulas from executing if the file is untrusted, or if the file is not authored by the current user. (Effectiveness: Limited)

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)

## Demonstrative Examples

**•** Stripping the leading equals sign, or simply not executing formulas from untrusted sources, impedes malicious activity.