# CWE Detail – CWE-526

## Description

The product uses an environment variable to store unencrypted sensitive information.

## Extended Description

Information stored in an environment variable can be accessible by other processes with the execution context, including child processes that dependencies are executed in, or serverless functions in cloud environments. An environment variable's contents can also be inserted into messages, headers, log files, or other outputs. Often these other dependencies have no need to use the environment variable in question. A weakness that discloses environment variables could expose this information.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Observed Examples (CVEs)

**•** CVE-2022-43691: CMS shows sensitive server-side information from environment variables when run in Debug mode.

**•** CVE-2022-27195: Plugin for an automation server inserts environment variable contents into build XML files.

**•** CVE-2022-25264: CI/CD tool logs environment variables related to passwords add Contribution to content history.

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

**•** Operation: N/A

## Common Consequences

**•** Impact: Read Application Data — Notes:

## Potential Mitigations

**•** Architecture and Design: Encrypt information stored in the environment variable to protect it from being exposed to an unauthorized user. If encryption is not feasible or is considered too expensive for the business use of the application, then consider using a properly protected configuration file instead of an environment variable. It should be understood that unencrypted information in a config file is also not guaranteed to be protected, but it is still a better choice, because it reduces attack surface related to weaknesses such as CWE-214. In some settings, vaults might be a feasible option for safer data transfer. Users should be notified of the business choice made to not protect the sensitive information through encryption. (Effectiveness: N/A)

**•** Implementation: If the environment variable is not necessary for the desired behavior, then remove it entirely, or clear it to an empty value. (Effectiveness: N/A)