# CWE Detail – CWE-220

## Description

The product stores sensitive data under the FTP server root with insufficient access control, which might make it accessible to untrusted parties.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Modes of Introduction

**•** Operation: N/A

**•** Architecture and Design: COMMISSION: This weakness refers to an incorrect design related to an architectural security tactic.

## Common Consequences

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

## Potential Mitigations

**•** Implementation: Avoid storing information under the FTP root directory. (Effectiveness: N/A)

**•** System Configuration: Access control permissions should be set to prevent reading/writing of sensitive files inside/outside of the FTP directory. (Effectiveness: N/A)

## Applicable Platforms

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