# Blue Team Essentials CVSS Calculator Capstone Scenario

**Adobe Acrobat Buffer Overflow Vulnerability (CVE-2009-0658)**

**Vulnerability**

Adobe Acrobat and Reader version 9.0 and earlier are vulnerable to a buffer overflow, caused by improper bounds checking when parsing a malformed JBIG2 image stream embedded within a PDF document. By persuading a victim to open a malicious PDF file, a remote attacker could overflow a buffer and execute arbitrary code on the system with the privileges of the victim or cause the application to crash.

**Attack**

The vulnerability is exploited by convincing a victim to open a malicious document on a system that uses a vulnerable version of Adobe Acrobat or Reader. An attacker must deliver a malicious document to the victim and relies upon the user to open it. Then the code execution achieved by the attacker depends on the privilege level of the user on the system and could potentially result in High impacts to Confidentiality, Integrity, and Availability.

**References**

**http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0658**

**http://www.adobe.com/support/security/advisories/apsa09-01.html**

**Example of CVSS Calculations**

CVSS v2.0 Calculator Example:

Base Score: 9.3

Metric Value

Access Vector: Network

Access Complexity: Medium

Authentication: None

Confidentiality Impact: Complete

Integrity Impact: Complete

Availability Impact: Complete

**CVSS v3.1**

**Base Score**: *7.8*

**Attack Vector:** *Local A flaw in the local document software that is triggered by opening a malformed document.*

**Attack Complexity:** *Low*

**Privileges Required:** *None*

**User Interaction Required:** *The victim needs to open the malformed document.*

**Scope:** *Unchanged*

**Confidentiality:** *High Assuming a worst-case impact of the victim having High privileges on the affected system.*

**Integrity:** *High Assuming a worst-case impact of the victim having High privileges on the affected system.*

**Availability:** *High Assuming a worst-case impact of the victim having High privileges on the affected system.*