Bug Report
Information Systems Security Analysis - CPSC 601.29

CAD-KAS PDF Reader Denial-of-Service Vulnerability

Vulnerable Systems

CAD-KAS PDF Reader 3.0

Summary

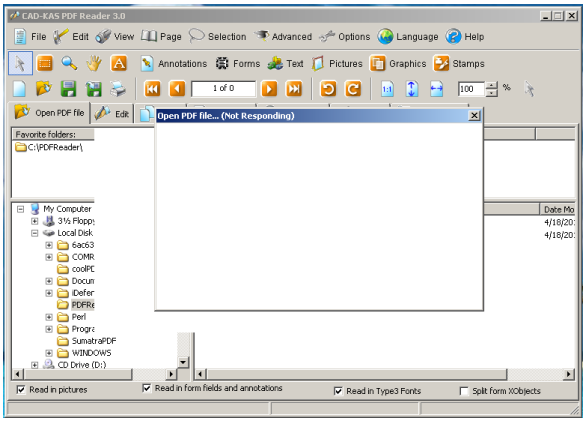
CAD-KAS PDF Reader is a MS Windows-based application to read PDF files. The application is affected by a denial-of-service vulnerability when handling certain PDF files.

Successful exploits may allow attackers to cause the application to hang.

Technical Description

CAD-KAS PDF Reader is a MS Windows-based application to read PDF files.

The vulnerability exists when the application handles a malformed PDF file with an object data block containing a certain tag followed by a large sequence of characters. The application fails to properly handle the string resulting in a denial-of-service condition. Analysis of the vulnerability shows that there are no overwrites of any memory control structures or a crash. Therefore, this issue is not exploitable to conduct any other attacks. The application code logic parses and moves individual Unicode bytes in a continuous loop which handles the string properly, but performs slowly particularly when handling an excessively large string. Initially thought to be an infinite loop, this process consumes the application's resources and response is denied to the user. There doesn't appear to be a cap on the length of this tag, so a large enough number of bytes will hang the application and trigger the Microsoft Windows Hungapp error to report that the application is not responding.



[Details Omitted]

Attack Scenario

Denial-of-Service

1. An attacker crafts a malicious file to exploit the affected application.
2. The attacker distributes the file through web, email or some other means.
3. The attacker entices unsuspecting to open the malicious file.
4. When the unsuspecting user opens the file, the application stops responding to user requests.

A successful exploit will allow an attacker to cause denial-of-service conditions. Users manipulating multiple PDF documents, upon opening the maliciously crafted will have to force quit the hung application.

Exploitability

Proof-of-Concept filename: target.pdf

Mitigating Strategies

Users should refrain from opening files originating from untrusted sources. This may include emails, websites or IM.

Solution

No fixes are currently available to address this issue.

Credit

This vulnerability and analysis was completed by Patrick Jungles.

References

Cad-Kas PDF Reader 3.0
http://www.cadkas.com/downengpdf5.php