



作者

CAST

**应用安全与开发的**

**安全技术实施指南**

**STIG Ver 4 Release 8**

**细节报告**

应用名称 –

分析版本 –

CAST AIP -

|  |
| --- |
|  |
|  |

我的应用名称

版本编号

我的CAST版本

# 目录

目录 2

1. 简介 3

1.1. 应用特征 3

2. 安全违规概述 4

STIG Ver 4 Release 8 Overview for ASD 4

2.1. STIG Ver 4 Release 8 CAT I 5

2.2. STIG Ver 4 Release 8 CAT II 6

2.3. STIG Ver 4 Release 8 CAT III 7

3. Security Violation Details 安全违规细节 8

3.1. STIG-V4R8-CAT1 –漏洞 8

3.2. STIG-V4R8 CAT-2 -漏洞 8

3.3. STIG-VR48 CAT-3 –漏洞 8

4. 附件 9

4.1. 关于CAST软件智能 9

4.2. 关于CAST安全 9

# 简介

此评估旨在确定应用的安全状况，并确定造成当前安全问题的根本原因，以及未来应用退化的风险。此评估使用CAST应用智能平台（AIP）根据STIG标准自动扫描应用介质，审查架构、设计和代码。

CAST AIP采用的质量规则来自行业流行的通用标准（OWASP、CWE、CISQ、STIG、PCI、NIST）。CAST具有执行数据流和系统级分析（从表示层到数据库层）的独特能力，提供最准确的安全性发现，减少误报。

## 应用特征

此评估重点关注所述应用（用户界面到数据库）的技术实现，而不分析业务功能。

|  |  |
| --- | --- |
| **Name** | **Value** |
| kLoC | 504 |
| Files | 6,586 |
| Classes | 593 |
| SQL Art. | 0 |
| Tables | 119 |

*图1：应用技术特征 表1：应用规模特征*

# 安全违规概述

本节总结了CAST AIP依据“应用安全与开发（ASD）的安全技术实施指南”进行结构质量分析和测量所识别的最严重的安全漏洞。

由国防信息系统局（DISA）开发并维护：控制相关的标识符（CCI）、安全需求指南（SRG）、安全技术实施指南（STIG）、以及移动代码风险类别和使用指南。以上指南执行并符合国防部网络安全政策、标准、架构、安全控制和验证程序。

STIG的发布和参考：国防部和联邦政府计算环境内的各方可从“信息保障支持环境”（IASE）网站获取适用的安全技术实施指南（STIG）。此网站包含所有STIG、SRG和其他相关的安全信息的最新副本。有关更多详细信息，请点击[STIG](http://iase.disa.mil/)。

## STIG Ver 4 Release 8 Overview for ASD

ASD STIG V4R8下CAST的适用范围。

**漏洞严重性分类码的定义**

严重性分类码（称为CAT）是用于评估设施或系统安全状态的漏洞度量。每个具体安全策略都被分配了一个严重性分类码：CAT I、CAT II或CAT III。

CAT I：漏洞一旦被利用，将立即直接导致机密性、可用性或完整性的损失。

CAT II：可能导致保密性、可用性或完整性丧失的漏洞。

CAT III：降低保护措施的保密性、可用性或完整性的漏洞。

|  |  |  |  |
| --- | --- | --- | --- |
| STIG V4R8 | Total Vulnerabilities | Added Vulnerabilities | Removed Vulnerabilities |
| Cat1 | 0 | 0 | 0 |
| Cat2 | 0 | 0 | 0 |
| Cat3 | 0 | 0 | 0 |

*表2：STIG V4R8 总结*

## STIG Ver 4 Release 8 CAT I

关于该应用的“STIG CAT I 违规”调查结果列表。

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Violations | Added Violations | Removed Violations |
| Rule 1 | 0 | 0 | 0 |
| Rule 2 | 0 | 0 | 0 |
| Rule 3 | 0 | 0 | 0 |
| Rule 4 | 0 | 0 | 0 |
| Rule 5 | 0 | 0 | 0 |
| Rule 6 | 0 | 0 | 0 |
| Rule 7 | 0 | 0 | 0 |
| Rule 8 | 0 | 0 | 0 |

*表3：* *STIG V4R8 CAT1 总结*

## STIG Ver 4 Release 8 CAT II

关于该应用的“STIG CAT II违规”调查结果列表。

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Violations | Added Violations | Removed Violations |
| Rule 1 | 0 | 0 | 0 |
| Rule 2 | 0 | 0 | 0 |
| Rule 3 | 0 | 0 | 0 |
| Rule 4 | 0 | 0 | 0 |
| Rule 5 | 0 | 0 | 0 |
| Rule 6 | 0 | 0 | 0 |
| Rule 7 | 0 | 0 | 0 |
| Rule 8 | 0 | 0 | 0 |

*表4：STIG V4R8 CAT2 总结*

## STIG Ver 4 Release 8 CAT III

关于该应用的“STIG CAT III违规”调查结果列表。

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Violations | Added Violations | Removed Violations |
| Rule 1 | 0 | 0 | 0 |
| Rule 2 | 0 | 0 | 0 |
| Rule 3 | 0 | 0 | 0 |
| Rule 4 | 0 | 0 | 0 |
| Rule 5 | 0 | 0 | 0 |
| Rule 6 | 0 | 0 | 0 |
| Rule 7 | 0 | 0 | 0 |
| Rule 8 | 0 | 0 | 0 |

*表5：STIG V4R8 CAT3总结*

# Security Violation Details 安全违规细节

## STIG-V4R8-CAT1 –漏洞

|  |
| --- |
| 违规 |
| 无违规项 |

## STIG-V4R8 CAT-2 -漏洞

|  |
| --- |
| 违规 |
| 无违规项 |

## STIG-VR48 CAT-3 –漏洞

|  |
| --- |
| 违规 |
| 无违规项 |

# 附件

## 关于CAST软件智能

软件智能通过系统分析数据库结构、软件框架和源代码，帮助团队更好地沟通、决策及驱动团队，保护企业和品牌，不断提高安全性和可靠性，更好地理解关键系统的复杂性。众多企业依靠CAST软件智能提高最终用户满意度，加快上市时间，防止业务中断并降低成本，克服现有障碍，成功应对创新挑战。

关于CAST软件智能更多相关信息，请访问<https://www.castsoftware.com/software-intelligence> 。

## 关于CAST安全

为了应对网络风险、保障应用安全，需要采取主动的、智能的方法措施。CAST软件智能够在开发开始前洞察安全策略盲点。凭借其独特的数据流和系统级分析能力，CAST提供最准确的安全性发现，减少误报。CAST安全规则源自行业最佳标准（CISQ、CWE和OWASP）。

了解更多CAST安全相关信息，请点击[此处](https://www.castsoftware.com/use-cases/application-security)。