

作者

CAST

**应用安全与开发**

**安全技术实施指南**

**STIG Ver 4 Release 8**

**合规报告**

应用名称 – 我的应用名称

分析版本 – 版本编号

CAST AIP - 我的CAST版本

|  |
| --- |
|  |
|  |

日期

# 目录

1. 简介

1.1. 应用特征

2. STIG Ver 4 Release 8 总结

2.1. STIG Ver 4 Release 8 漏洞总结

3. STIG Ver 4 Release 8 CAT I - CAST分析发现

4. STIG Ver 4 Release 8 CAT II- CAST分析发现

5. STIG Ver 4 Release 8 CAT III- CAST分析发现

6. 附录

6.1. 关于CAST软件智能

6.2. 关于CAST安全性

6.3. STIG Ver 4 Release 8 在CAST 方案中的适用性

# 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，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

本评估重点关注所述应用（用户界面到数据库）的技术实现，不分析业务功能。

|  |  |
| --- | --- |
| **名称** | **值** |
| 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*

# STIG Ver 4 Release 8 总结

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

由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。以上指南符合DoD网络安全政策、标准、架构、安全控制和验证程序。

STIG的分布与来源：DoD计算环境内的各方可从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 漏洞总结

**漏洞严重性分类码定义**

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分析方法。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。

**ASD STIG V4R8——CAST分析发现**

| STIG V4R8 | 总漏洞 | 新增漏洞 | 移除漏洞 |
| --- | --- | --- | --- |
| Cat1 | 0 | 0 | 0 |
| Cat2 | 0 | 0 | 0 |
| Cat3 | 0 | 0 | 0 |

*表2: STIG V4R8 总结*

**ASD STIG V4R8及其亚级标准——CAST分析发现**

| STIG V4R8 | 总漏洞 | 新增漏洞 | 移除漏洞 |
| --- | --- | --- | --- |
| Cat1 | 0 | 0 | 0 |
| Cat2 | 0 | 0 | 0 |
| Cat3 | 0 | 0 | 0 |

*表3: STIG V4R8 概览*

# STIG Ver 4 Release 8 CAT I - CAST分析发现

STIG CAT I——CAST识别漏洞

| 规则 | 总漏洞 | 新增漏洞 | 移除漏洞 |
| --- | --- | --- | --- |
| 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 CAT1 总结*

# STIG Ver 4 Release 8 CAT II- CAST分析发现

STIG CAT II——CAST识别漏洞

| 规则 | 总漏洞 | 新增漏洞 | 移除漏洞 |
| --- | --- | --- | --- |
| 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 CAT2 总结*

# STIG Ver 4 Release 8 CAT III- CAST分析发现

STIG CAT III——CAST识别漏洞

| 规则 | 总漏洞 | 新增漏洞 | 移除漏洞 |
| --- | --- | --- | --- |
| 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6: STIG V4R8 CAT3 总结*

# 附录

## 关于CAST软件智能

软件智能提供软件架构、端到端事务流、数据访问模式等方面的深刻洞察力，帮助提高IT团队工作效率。CAST软件智能已成功帮助数百家国际知名企业改善其最终用户满意度、加快其产品上市时间、防止业务中断并有效降低成本，使企业级客户能够克服技术障碍、成熟应对创新潮流。

了解更多CAST软件智能相关信息，请点击[此处](https://www.castsoftware.com/)。

## 关于CAST安全性

应对网络风险，保障应用安全，需采取主动的、智能的方法。CAST 软件智能帮助团队在开始开发前深入探索发现应用的架构安全盲点。凭借其独特的数据流分析和系统级别分析能力，CAST提供最准确的安全发现，减少安全误报。CAST安全规则来自一流的行业标准——CISQ, CWE, OWASP, PCI-DSS, NIST, STIG。了解CAST安全性的更多信息，请点击[此处](https://www.castsoftware.com/products/security-dashboard) 。

## STIG Ver 4 Release 8 在CAST 方案中的适用性

| 标准 | 描述 | 适用性 |
| --- | --- | --- |
| Cat1 | 0 | 0 |
| Cat2 | 0 | 0 |
| Cat3 | 0 | 0 |