

log4jj bizarre adventure



Dio Stonemask Inc.

Penetration Test Report of Findings

Jojo

2022-08-10T14:47:40.140406Z

Version 1.0



State of Confidentiality

Executive Summary

Assessment Overview and Recommendations

Number of Findings per Category

Severity Overview of Findings

Technical Findings and Comments Details

INFORMATION_GATHERING OTG-INFO-001

INFORMATION_GATHERING OTG-INFO-002

Appendencies

Findings Severities

Risk Matrix

Severity Rating Definitions



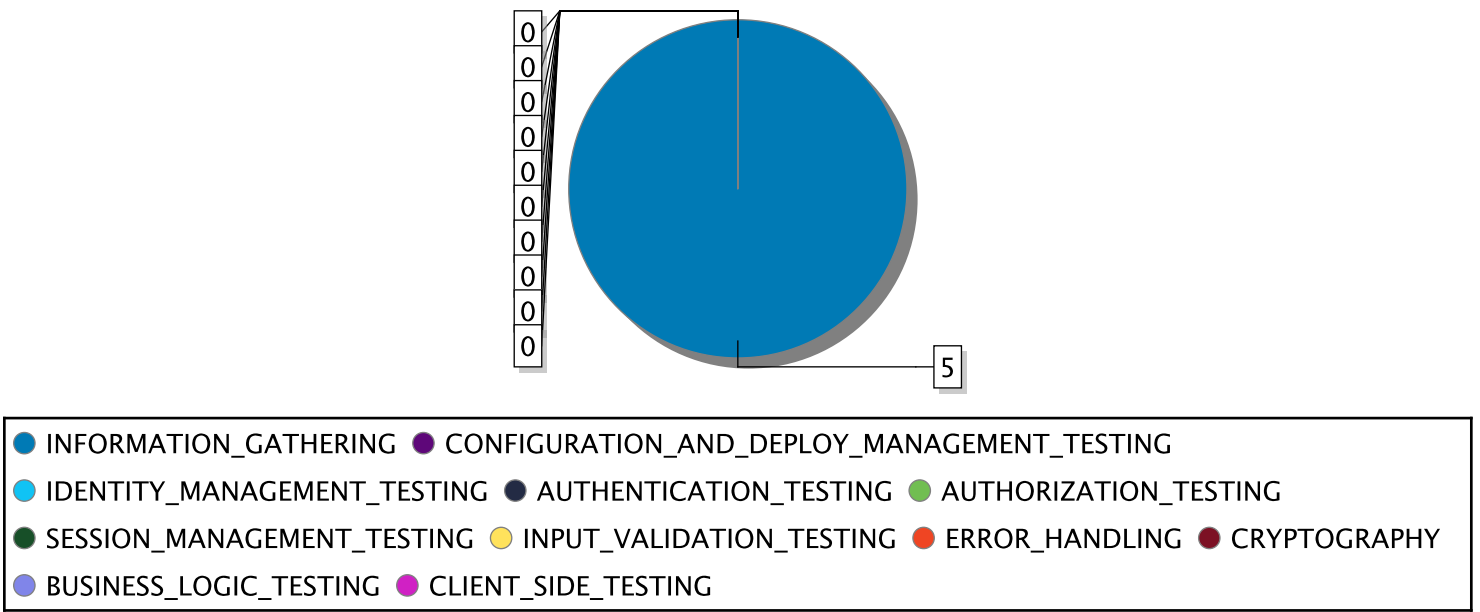
The contents of this document have been developed by Jojo. Jojo considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Jojo. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Jojo.

The contents of this document do not constitute legal advice. Jojo's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against the company Dio Stonemask Inc. for examination purposes, and the vulnerabilities included in this document should be mitigated in order to secure Dio Stonemask Inc. external or internal infrastructure.

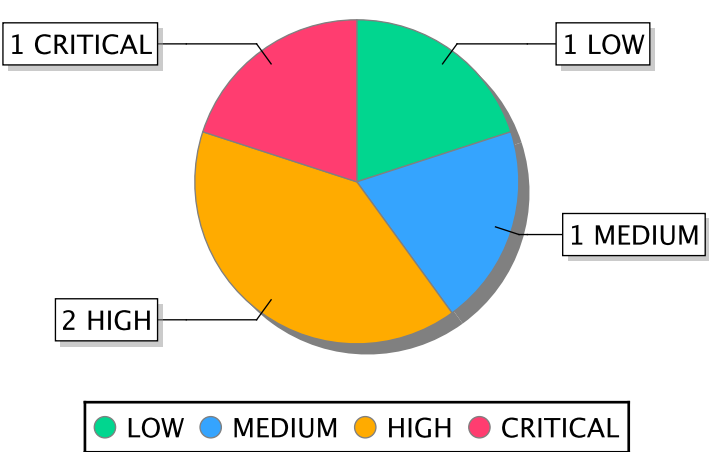
Assessment Overview and Recommendations

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue dui dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet.

Number of Findings per Category



Severity Overview of Findings



**Finding:** ef31449d-71ec-4736-952f-8b20e53117d5**Title:**

Test Title

LOW

Description:

Test Description Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut tristique sodales leo, eget porta dolor porttitor vitae. Nunc semper a est in porttitor. Aliquam imperdiet mi eget orci egestas euismod. Fusce sit amet massa efficitur, egestas neque vitae, elementum orci. Nullam accumsan nunc id risus volutpat, quis sagittis lorem sollicitudin. Nam finibus justo non arcu vulputate dignissim. Etiam libero felis, dignissim non feugiat at, ornare non elit. Sed hendrerit risus id magna porttitor interdum. Cras vehicula odio id metus elementum porta. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Curabitur tempor eu purus ut aliquet. Nam.

Impact:

Test Impact Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut tristique sodales leo, eget porta dolor porttitor vitae. Nunc semper a est in porttitor. Aliquam imperdiet mi eget orci egestas euismod. Fusce sit amet massa efficitur, egestas neque vitae, elementum orci. Nullam accumsan nunc id risus volutpat, quis sagittis lorem sollicitudin.

Reproduction Steps:

Step 1: Test

Mitigation:

No mitigation to avoid, minimize or compensate the finding found or needed.

Affected URL's:

<https://akveo.github.io/nebular/docs/components/progress-bar/examples#nbprogressbarcomponent>, <https://www.google.de/>

Finding: 58f63b4e-97fb-4fe8-8527-7996896089d2

Title:

Medium Finding

MEDIUM

Description:

Medium Description Nam finibus justo non arcu vulputate dignissim. Etiam libero felis, dignissim non feugiat at, ornare non elit. Sed hendrerit risus id magna porttitor interdum. Cras vehicula odio id metus elementum porta. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Curabitur tempor eu purus ut aliquet.

Impact:

Medium Impact

Reproduction Steps:

Step 1: Medium

Mitigation:

Fusce sit amet massa efficitur, egestas neque vitae, elementum orci. Nullam accumsan nunc id risus volutpat, quis sagittis lorem sollicitudin. Nam finibus justo non arcu vulputate dignissim. Etiam libero felis, dignissim non feugiat at, ornare non elit. Sed hendrerit risus id magna porttitor interdum.

Affected URL's:

No specific URL's affected.

Finding: 58f63b4e-97fb-4fe8-8527-7996896089d2

Title:

High Finding

HIGH

Description:

High Description Nam finibus justo non arcu vulputate dignissim. Etiam libero felis, dignissim non feugiat at, ornare non elit. Sed hendrerit risus id magna porttitor interdum. Cras vehicula odio id metus elementum porta. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Curabitur tempor eu purus ut aliquet.

Impact:

High Impact

Reproduction Steps:

Step 1: High

Mitigation:

No mitigation to avoid, minimize or compensate the finding found or needed.

Affected URL's:

No specific URL's affected.

Finding: 58f63b4e-97fb-4fe8-8527-7996896089d2

Title:

Critical Finding

CRITICAL

Description:

Critical Description Nam finibus justo non arcu vulputate dignissim. Etiam libero felis, dignissim non feugiat at, ornare non elit. Sed hendrerit risus id magna porttitor interdum. Cras vehicula odio id metus elementum porta. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Curabitur tempor eu purus ut aliquet.

Impact:

Critical Impact

Reproduction Steps:

Step 1: Critical

Mitigation:

Fusce sit amet massa efficitur, egestas neque vitae, elementum orci. Nullam accumsan nunc id risus volutpat, quis sagittis lorem sollicitudin. Nam finibus justo non arcu vulputate dignissim. Etiam libero felis, dignissim non feugiat at, ornare non elit. Sed hendrerit risus id magna porttitor interdum.

Affected URL's:

<https://community.jaspersoft.com/system/files/restricted-docs/jaspersoft-studio-user-guide.pdf>

Comment: 89703b19-16c7-49e5-8e33-0c706313e5fe

Title:

Test Comment

Description:

Not related to findings

Comment: 89703b19-16c7-49e5-8e33-0c706313e5fe

Title:

Test Comment

Description:

Test Decription



Finding: 4ddb84f6-068c-4319-a8ee-100008bb75a

Title:

Anothe High Issues

HIGH

Description:

High

Impact:

High

Reproduction Steps:

High

Mitigation:

No mitigation to avoid, minimize or compensate the finding found or needed.

Affected URL's:

No specific URL's affected.

Comment: 89703b19-16c7-49e5-8e33-0c706313e5fe

Title:

Test Comment

Description:

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua.



Findings Severities

Each finding has been assigned a severity rating of critical high, medium, or low. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability.

Risk Matrix

The risk matrix is used to assess the potential damage of a hazard, based on the likelihood and severity factors. The likelihood and severity scores are multiplied to obtain a score value. This score is looked up in the risk ranges to determine the risk level. An example of a hazard risk matrix is given below:

Risk score	Risk level category	<i>Likelihood</i>				
1 to 4	Low					
5 to 10	Medium					
11 to 18	High	Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Almost certain (5)
19 to 25	Critical					
<i>Severity</i>	Catastrophic (5)	Medium	Medium	High	Critical	Critical
	Major (4)	Low	Medium	High	High	Critical
	Moderate (3)	Low	Medium	Medium	High	High
	Minor (2)	Low	Low	Medium	Medium	Medium
	Insignificant (1)	Low	Low	Low	Low	Medium

Example, if Likelihood = Possible (3) and Severity = Major (4), the risk level is determined by severity * likelihood, which is $3 \times 4 = 12$. The score 12 falls in 'High' risk range.

Rating	Severity Rating Definition
Critical	Exploitation of the technical or procedural vulnerability will cause substantial harm. Significant political, financial, and/or legal damage is likely to result. The threat exposure is critical, and a publicly available mechanism exists to exploit the vulnerability. Security controls are not effectively implemented to reduce the severity of impact if the vulnerability were exploited.
High	Exploitation of the technical or procedural vulnerability will cause substantial harm. Significant political, financial, and/or legal damage is likely to result. The threat exposure is high, thereby increasing the likelihood of occurrence. Security controls are not effectively implemented to reduce the severity of impact if the vulnerability were exploited.
Medium	<p>Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity, and/or availability of the system, application, or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment. The threat exposure is moderate-to-high, thereby increasing the likelihood of occurrence. Security controls are in place to contain the severity of impact if the vulnerability were exploited, such that further political, financial, or legal damage will not occur.</p> <p>- OR -</p> <p>The vulnerability is such that it would otherwise be considered High Risk, but the threat exposure is so limited that the likelihood of occurrence is minimal.</p>
Low	<p>Exploitation of the technical or procedural vulnerability will cause minimal impact to operations. The Confidentiality, Integrity and Availability (CIA) of sensitive information are not at risk of compromise.</p> <p>Exploitation of the vulnerability may cause slight financial loss or public embarrassment. The threat exposure is moderate-to-low. Security controls are in place to contain the severity of impact if the vulnerability were exploited, such that further political, financial, or legal damage will not occur.</p> <p>- OR -</p> <p>The vulnerability is such that it would otherwise be considered Medium Risk, but the threat exposure is so limited that the likelihood of occurrence is minimal.</p>