Secure Lab 12

VULNERABILITY REPORT

FRIDAY, JUNE 11, 2021

MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	06/11/2021	S V Girish Kumar	Initial Version

TABLE OF CONTENTS

GENERAL INFORMATION

SCOPE

VIT-AP has mandated us to perform security tests on the following scope:

ORGANISATION

The testing activities were performed between 06/11/2021 and 06/12/2021.

EXECUTIVE SUMMARY

VULNERABILITIES SUMMARY

Following vulnerabilities have been discovered:

Risk	ID	Vulnerability	Affected Scope
High	IDX-003	DOMXSS	
High	IDX-001	Buffer Overflow	
High	IDX-002	Clickjacking	

TECHNICAL DETAILS

DOMXSS

CVSS SEVERITY	**High**		**CVSSV3 SCORE**	**7.9**
CVSSV3 CRITERIAS	Attack Vector :	**Network**	Scope :	**Changed**
	Attack Complexity :	**High**	Confidentiality :	**High**
	Required Privileges :	**Low**	Integrity :	**High**
	User Interaction :	**Required**	Availability :	**Low**
AFFECTED SCOPE				
DESCRIPTION	DOM-based XSS vulnerabilities usually arise when JavaScript takes data from an attacker-controllable source, such as the URL, and passes it to a sink that supports dynamic code execution, such as `eval()` or `innerHTML`. This enables attackers to execute malicious JavaScript, which typically allows them to hijack other users' accounts. To deliver a DOM-based XSS attack, you need to place data into a source so that it is propagated to a sink and causes execution of arbitrary JavaScript.			
OBSERVATION				
TEST DETAILS				
REMEDIATION				
REFERENCES				

BUFFER OVERFLOW

CVSS SEVERITY	**High**		**CVSSV3 SCORE**	**7.5**
CVSSV3 CRITERIAS	Attack Vector :	**Local**	Scope :	**Changed**
	Attack Complexity :	**High**	Confidentiality :	**High**
	Required Privileges :	**Low**	Integrity :	**High**
	User Interaction :	**Required**	Availability :	**High**
AFFECTED SCOPE				
DESCRIPTION	A buffer overflow occurs when the data that is written into the buffer exceeds the allocated space and results in the overwriting of adjacent memory locations. Security attacks using buffer overflow are fairly common and most of them seek to modify data in the memory, gain access to confidential data and many more similar exploits.			
OBSERVATION				
TEST DETAILS				
REMEDIATION				
REFERENCES				

CLICKJACKING

CVSS SEVERITY	**High**		**CVSSV3 SCORE**	**7.5**
CVSSV3 CRITERIAS	Attack Vector :	**Network**	Scope :	**Changed**
	Attack Complexity :	**Low**	Confidentiality :	**High**
	Required Privileges :	**High**	Integrity :	**Low**
	User Interaction :	**Required**	Availability :	**Low**
AFFECTED SCOPE				
DESCRIPTION	Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online. Typically, clickjacking is performed by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees. The user believes they are clicking the visible page but in fact they are clicking an invisible element in the additional page transposed on top of it.			
OBSERVATION				
TEST DETAILS				
REMEDIATION				
REFERENCES				