

Charitha

VULNERABILITY REPORT

10-06-2021

MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	10-06-2021	Charitha Bodapothula	Initial Version

TABLE OF CONTENTS

1.	General Information	4
1.1	Scope	4
1.2	Organisation.....	4
2.	Executive Summary.....	5
3.	Technical Details.....	6
3.1	title	Error! Bookmark not defined.
4.	Vulnerabilities summary	6

GENERAL INFORMATION

SCOPE

SC_LAB has mandated us to perform security tests on the following scope:

ORGANISATION

The testing activities were performed between 10-06-2021 and 13-06-2021.

EXECUTIVE SUMMARY

VULNERABILITIES SUMMARY

Following vulnerabilities have been discovered:

Risk	ID	Vulnerability	Affected Scope
Medium	VULN-001	.NET Framework Denial of Service Vulnerability	<div><div>Issue: 001001010 CVE: CVE-2012-14111 ID: 000000000 Title: .NET Framework Denial of Service Vulnerability Affected product: Microsoft .NET Framework 4.0 on Windows 10 version 2802 for x64-based Systems Affected component: IIS/MS OLE Security: Disruption Impact: Denial of Service Priority: P-4</div></div>
Medium	VULN-003	.NET Framework Denial of Service Vulnerability -2	<div><div>Issue: 001001010 CVE: CVE-2012-14111 ID: 000000000 Title: .NET Framework Denial of Service Vulnerability Affected product: Microsoft .NET Framework 4.0 on Windows 10 version 2802 for x64-based Systems Affected component: IIS/MS OLE Security: Disruption Impact: Denial of Service Priority: P-4</div></div>

TECHNICAL DETAILS

.NET FRAMEWORK DENIAL OF SERVICE VULNERABILITY

CVSS SEVERITY	Medium	CVSSv3 SCORE	6.2
CVSSv3 CRITERIAS	Attack Vector : Network	Scope : Unchanged	
	Attack Complexity : High	Confidentiality : Medium	
	Required Privileges : Low	Integrity : Low	
	User Interaction : Required	Availability : High	
AFFECTED SCOPE			
DESCRIPTION	A denial-of-service vulnerability exists when .NET Core or .NET Framework improperly handles web requests. An attacker who successfully exploited this vulnerability could cause a denial of service against a .NET Core or .NET Framework web application. The vulnerability can be exploited remotely, without authentication		
OBSERVATION	The vulnerability exists when Microsoft .NET Framework hashes specially crafted requests and inserts that data into a hash table, causing a hash collision . When many of these collisions are chained together, the performance of the hash table is greatly degraded, leading to the denial-of-service condition.		
<div>TEST DETAILS</div> <div>Date: 20210216 CVE: CVE-2021-24111 KB: KB4601050 Title: .NET Framework Denial of Service Vulnerability Affected product: Microsoft .NET Framework 4.8 on Windows 10 Version 20H2 for x64-based Systems Affected component: Issuing CNA Severity: Important Impact: Denial of Service Exploit: n/a</div>			
REMEDIATION	Microsoft .NET Framework Denial of Service Vulnerability (KB4603002) (mageni.net)		
REFERENCES	https://hackerone.com/reports/485748		

.NET FRAMEWORK DENIAL OF SERVICE VULNERABILITY-2.NET FRAMEWORK DENIAL OF SERVICE VULNERABILITY

CVSS SEVERITY	Medium	CVSSv3 SCORE	4.5
CVSSv3 CRITERIAS	Attack Vector : Physical	Scope : Unchanged	
	Attack Complexity : High	Confidentiality : None	
	Required Privileges : Low	Integrity : Low	
	User Interaction : Required	Availability : High	
AFFECTED SCOPE			
DESCRIPTION	A denial-of-service vulnerability exists when .NET Core or .NET Framework improperly handles web requests. An attacker who successfully exploited this vulnerability could cause a denial of service against a .NET Core or .NET Framework web application. The vulnerability can be exploited remotely, without authentication		
OBSERVATION	The vulnerability exists when Microsoft .NET Framework hashes specially crafted requests and inserts that data into a hash table, causing a hash collision . When many of these collisions are chained together, the performance of the hash table is greatly degraded, leading to the denial-of-service condition.		
<div>TEST DETAILS</div> <div>Date: 20210216 CVE: CVE-2021-24111 KB: KB4601050 Title: .NET Framework Denial of Service Vulnerability Affected product: Microsoft .NET Framework 4.8 on Windows 10 Version 20H2 for x64-based Systems Affected component: Issuing CNA Severity: Important Impact: Denial of Service Exploit: n/a</div>			
REMEDIATION	Microsoft .NET Framework Denial of Service Vulnerability (KB4603002) (mageni.net)		
REFERENCES	https://hackerone.com/reports/485748		

