Arsharth.P

VULNERABILITY REPORT

10-06-2021

MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	10-06-2021	Arsharth.P	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:

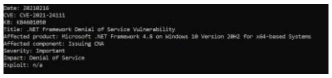
Organisation

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

Executive Summary

VULNERABILITIES SUMMARY

Following vulnerabilities have been discovered:

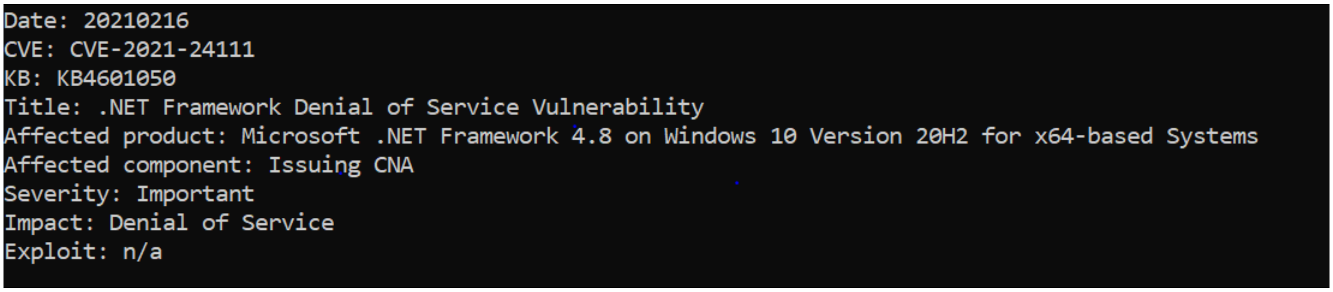
Risk	ID	Vulnerability	Affected Scope
Medium	VULN-001	.NET Framework Denial of Service Vulnerability	 Date: 20210216 CVE: CVE-2021-24111 KB: KB4601050 Title: .NET Framework Denial of Service Vulnerability Affected product: Microsoft .NET Framework 4.8 on Windows 10 Version 20H2 for x64-based Systems Affected component: Issuing CNA Severity: Important Impact: Denial of Service Exploit: n/a

Technical Details

.NET Framework Denial of Service Vulnerability

CVSS Severity	**Mediu m**		**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 Frameworkweb 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 ofthese collisions are chained together, the performance of the hash table is greatly degraded, leading to the denial-of-service condition.			

Test details



```
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
```

Remediation	Microsoft .NET Framework Denial of Service Vulnerability (KB4603002)(mageni.net)
References	https://hackerone.com/reports/485748