

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 10-06-2021 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	<pre>CVE-2019-0854 CVE-2019-0855 CVE-2019-0856 CVE-2019-0857 CVE-2019-0858 CVE-2019-0859 CVE-2019-0860 CVE-2019-0861 CVE-2019-0862 CVE-2019-0863 CVE-2019-0864 CVE-2019-0865 CVE-2019-0866 CVE-2019-0867 CVE-2019-0868 CVE-2019-0869 CVE-2019-0870 CVE-2019-0871 CVE-2019-0872 CVE-2019-0873 CVE-2019-0874 CVE-2019-0875 CVE-2019-0876 CVE-2019-0877 CVE-2019-0878 CVE-2019-0879 CVE-2019-0880 CVE-2019-0881 CVE-2019-0882 CVE-2019-0883 CVE-2019-0884 CVE-2019-0885 CVE-2019-0886 CVE-2019-0887 CVE-2019-0888 CVE-2019-0889 CVE-2019-0890 CVE-2019-0891 CVE-2019-0892 CVE-2019-0893 CVE-2019-0894 CVE-2019-0895 CVE-2019-0896 CVE-2019-0897 CVE-2019-0898 CVE-2019-0899 CVE-2019-0900 CVE-2019-0901 CVE-2019-0902 CVE-2019-0903 CVE-2019-0904 CVE-2019-0905 CVE-2019-0906 CVE-2019-0907 CVE-2019-0908 CVE-2019-0909 CVE-2019-0910 CVE-2019-0911 CVE-2019-0912 CVE-2019-0913 CVE-2019-0914 CVE-2019-0915 CVE-2019-0916 CVE-2019-0917 CVE-2019-0918 CVE-2019-0919 CVE-2019-0920 CVE-2019-0921 CVE-2019-0922 CVE-2019-0923 CVE-2019-0924 CVE-2019-0925 CVE-2019-0926 CVE-2019-0927 CVE-2019-0928 CVE-2019-0929 CVE-2019-0930 CVE-2019-0931 CVE-2019-0932 CVE-2019-0933 CVE-2019-0934 CVE-2019-0935 CVE-2019-0936 CVE-2019-0937 CVE-2019-0938 CVE-2019-0939 CVE-2019-0940 CVE-2019-0941 CVE-2019-0942 CVE-2019-0943 CVE-2019-0944 CVE-2019-0945 CVE-2019-0946 CVE-2019-0947 CVE-2019-0948 CVE-2019-0949 CVE-2019-0950 CVE-2019-0951 CVE-2019-0952 CVE-2019-0953 CVE-2019-0954 CVE-2019-0955 CVE-2019-0956 CVE-2019-0957 CVE-2019-0958 CVE-2019-0959 CVE-2019-0960 CVE-2019-0961 CVE-2019-0962 CVE-2019-0963 CVE-2019-0964 CVE-2019-0965 CVE-2019-0966 CVE-2019-0967 CVE-2019-0968 CVE-2019-0969 CVE-2019-0970 CVE-2019-0971 CVE-2019-0972 CVE-2019-0973 CVE-2019-0974 CVE-2019-0975 CVE-2019-0976 CVE-2019-0977 CVE-2019-0978 CVE-2019-0979 CVE-2019-0980 CVE-2019-0981 CVE-2019-0982 CVE-2019-0983 CVE-2019-0984 CVE-2019-0985 CVE-2019-0986 CVE-2019-0987 CVE-2019-0988 CVE-2019-0989 CVE-2019-0990 CVE-2019-0991 CVE-2019-0992 CVE-2019-0993 CVE-2019-0994 CVE-2019-0995 CVE-2019-0996 CVE-2019-0997 CVE-2019-0998 CVE-2019-0999 CVE-2020-0000</pre>

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.			
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			

