Stream Ripper 32 & Frigate

VULNERABILITY REPORT

MONDAY, MAY 25, 2021







MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	05/17/2021	G.Gayathri	Initial Version

CONFIDENTIAL



TABLE OF CONTENTS

I. General Information	4
1.1 Scope	4
1.2 Organisation	4
2. Executive Summary	5
3. Technical Details	6
3.1 title	6
1. Vulnerabilities summary	8





GENERAL INFORMATION

S_{COPE}

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

• Software Security

ORGANISATION

The testing activities were performed between 05/17/2021 and 05/17/2021.



EXECUTIVE SUMMARY





Vulnerabilities summary

Following vulnerabilities have been discovered:

Risk	ID	Vulnerability	Affected Scope
High	IDX-002	Shell Code Injection	Frigate
Medium	VULN-001	Buffer Overflow	StreamRipper 32 and Frigate



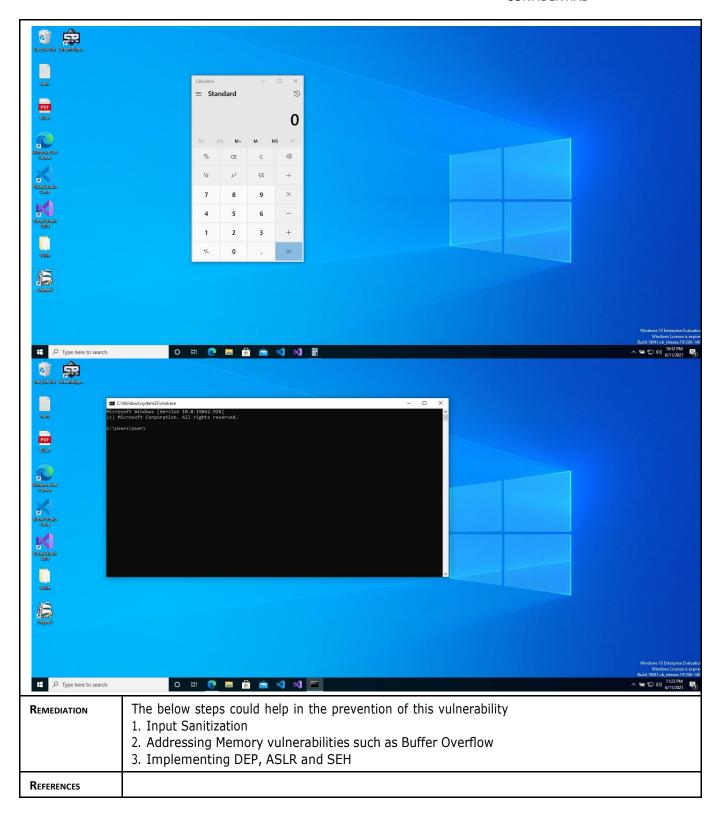
TECHNICAL DETAILS

SHELL CODE INJECTION

VSS SEVERITY		HIG	H		CVSSv3 Score		8.0
VSSv3 criterias	Attack Vector	:	Networ	·k	Scope :	Changed	
	Attack Comple	exity :	High		Confidentiality:	High	
	Required Privi	ileges :	Low		Integrity:	High	
	User Interaction	on:	Require	ed	Availability :	High	
FFECTED SCOPE	Frigate						
ESCRIPTION	The hacker codes. The	r infiltrate hacker ca	s the vu in easily	Inerable produced the control of the	ique where the hack ograms and makes t execute any kind of r attacks such as da omware attacks.	hem execute the code from a vul	eir own malicious nerable field thus
BSERVATION		field thus	leading	to many h	to exploit an applica narmful unwanted ac	tivities such as o	data loss or leak,
SCT DETAILS		ransom	ware atta	acks, privile	ege escalation and ev	en system take	over
EST DETAILS Frigate 3.36 ile Command Disk Utilities Manager Pac New - Ø Yew - Ø Edit - Ø Refresh Ø	Ø Copy Move ➤ Delete Renar □ Stop					ven system take	- g
Frigate 3.36 file Command Disk Utilities Manager Pag New - ② Yew - ② Yew - ② Yef dit - ② Refresh \ \[\frac{1}{2} \] \frac{1}{2} \] \(\frac{1}{2} \) \(\fr	Ø Copy 🔊 Move 🔀 Delete 🔟 Renar □ Stop ste Features.htm	me 🔆 Select • 🎪 Favorite	s • 🔯 Search 💍 FTP	Pack Properties Properties List - Name -	Obstoc COProgram Fles (165) Frigate(3)	ven system take	Add QuickLaunch 22
Frigate 1.36 New - 2 View - 2 Edn - 2 Refresh New - 3 View - 3 Edn - 3 Refresh New - 3 View - 3 Edn - 3 Refresh New - 3 View - 3 Edn - 3 Refresh New - 3 Edn - 3	Move to Delete Renar Stop LiveKernelReports Logs Media Microsoft.NET Migration ModemLogs OCR Se QLOffline Web Pages Panther Performance PIA PolisyPefinitions	System32 System32 SystemApps SystemResources SysWON64 TAPI Tesks Temp tracing twain 32 Ves Web	s • 🔯 Search 💍 FTP Search 💍 FTP Search 💍 FTP	Ust - Name - dll ini cll.Manifests late log prx	CoProgram Flacs (ASS) Frigate(3). K Addons Data Help Plugins For exe Juninacolo exe databate dil databath him	ven system take	Add Quick Launch 22
Frigate 136 The Manager Page 16 Command Disk Utilities Manager M	Move Clete Renary Defended Renary LiveKernelReports Logs Wedia Wicrosoft.NET Wigration ModesLogs OCR Parther Performance PIA	me System32 System32 SystemAppa SystemAppa SysteM64 SystemAppa Tapk Tapk Tapk Tapp Uvas Waas Wab Winsx ■ bfave Webplorer Welplane	s • 🐼 Search 🐧 FTP @ twain 32 @ win Windows5h @ Windows5h	Pack Properties Dark List * Name * dil	COProgram Fies 0-55 A Fragate 3) K Addons Data	en system take	Add QuickLaunch 22
Fright=136 ile Command Disk Utilities Manager Page 1 New - 2 View - # Edit - 2 Refresh Page 1 - 2 S	© Copy Move	System32 System32 SystemAppa SystemAppa SystemAppa SystemAppa SystemAppa TAPI Tasks Temp tracing train_32 Vas Wab Wab Wab WinSxS Infave Replorer	Search FIP Twain 32 Twain 32 WindowsShr WindowsShr WindowsShr WindowsShr WindowsShr WindowsShr WindowsShr WindowsShr WindowsShr	Pack Properties Properties Properties	CCProgram Fies (268) Frigate3). K Addons Data Help Plugins Et Et Strigate3 Gamman000 Addons Include Addons	ven system take	Add Quick Launch 22 46
Frigate 136 The Memory Diew Wilson Manager Page 166 New - @ View Wilson Memory Page 166 Fre Memory Memor	Determine Move Determine Movement Supports LiveKernelReports LiveKernelReports LiveKernelReports LiveKernelReports LiveKernelReports LiveKernelReports LiveKernelReports Microcoft.NET M	System32 System32 System32 SystemAppa SystemSeources SystwW64 TAPI Tasks Temp tracing tracing train, 32 Vas Mab Winsxs Ibfave WelpFane Minsxs Ibfave MelpFane MelpFan	Exe Exe Exe Exe Exe Exe Exe Exe	Pack Properties Properties Properties	CCProgram Fies (268) Frigate3). K Addons Data Help Plugins Figure Figure Cake Surget	ven system take	Add QuickLaunch 22
Fright 136 ile Command Disk Utilities Manager Page 1 New - 2 View - 2 Edit - 2 Edited - 2 File Manager 2 File Manager 2 A View - 3 Sa	© Copy Move	System32 SystemApps SystemApps SystemApps SystemApps SystemApps SystemApps SystemApps TAPI Tasks Temp Tracing Twain 32 Ves Wass Medb Winsxs Spirace Winsxs Spirace Winsxs Spirace SystemApps System Sy	exe	Pack Properties Properties Properties	CCProgram Fies (268) Frigate3). K Addons Data Help Plugins Figure Figure Cake Surget	ven system take	Add QuickLaunch 22
Frigate 136 The Manager Page 166 Command Disk Utilities Manager Manag	Determined the control of the contro	System32 System42 Sys	exe	Pack Properties Properties Properties	CCProgram Fies (268) Frigate3). K Addons Data Help Plugins Figure Figure Cake Surget	en system take	Add Quicklaunch 22

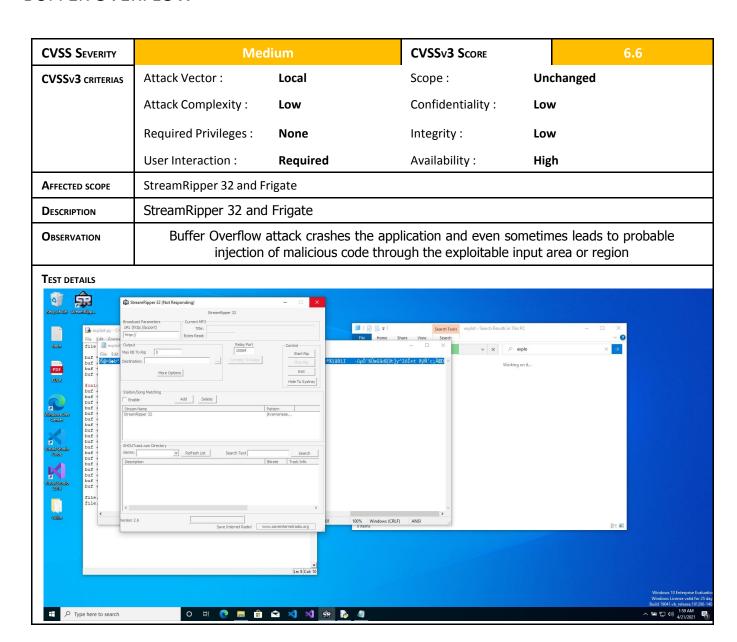








BUFFER OVERFLOW





CONFIDENTIAL

