Reporte de Vulnerabilidad

Document Creator	Omar Alejandro Hinojosa Ochoa
Revision	1
Last updated	07/12/2023
Owner	
Reviewer	

Contents

Findings	2
Critical severity vulnerabilities	2
Evidencia	2
High severity vulnerabilities	3
Evidencia	3
Mid severity vulnerabilities	5
Evidencia	5
Low severity vulnerabilities	6
Evidencia	7
Summary	8

Findings

Critical severity vulnerabilities

SEVERITY: Critical

No fueron detectadas vulnerabilidades de severidad critica en el escaneo del proyecto.

Evidencia:

1.



Recommendations

• La gestión de vulnerabilidades crítica es una parte crucial de la seguridad de cualquier sistema o aplicación.

Por lo tanto, debemos priorizar estas vulnerabilidades.

High severity vulnerabilities

SEVERITY: High

Un constructor estático es un tipo especial de constructor que se utiliza para inicializar cualquier dato estático o realizar otras tareas que deben ejecutarse una sola vez cuando la clase se carga por primera vez en la memoria. Los constructores estáticos no pueden tener modificadores de acceso y se ejecutan antes de que se acceda a cualquier miembro estático de la clase o se crea una instancia de la clase.

Evidencia:

```
ProyectoFinal_HOOA Program.cs

1 omar...
2 using System;
using System.Security.Cryptography;
using System.Text;
using System.To;

class Program

Add a 'protected' constructor or the 'static' keyword to the class declaration.

Move 'Program' into a named namespace.
```

Solucion:

Recommendations

• Los constructores permiten inicializar los miembros de una clase cuando se crea una instancia. Esto es esencial para que los objetos tengan un estado valida desde el principio.

Mid severity vulnerabilities

SEVERITY: Medium

El código obsoleto se refiere a partes de un programa que han sido marcadas como desaconsejadas o en desuso. Aunque el código obsoleto sigue siendo funcional, no es recomendable seguir utilizándolo.

Evidencia:

2.

3.

```
using (Aes aesCrip = Aes.Create())
{
    aesCrip.Key = clave;
    aesCrip.IV = iv;
    aesCrip.Mode = CipherMode.CBC;
    aesCrip.Padding = PaddingMode.PKCS7;

    using (MemoryStream ms = new MemoryStream())
{
        using (CryptoStream cs = new CryptoStream(ms, aesCrip.CreateEncryptor(), CryptoStreamMode.Write))
        {
            byte[] textoBytes = Encoding.UTF8.GetBytes(texto);
            cs.Write(textoBytes, 0, textoBytes.Length);
        }
        return Convert.ToBase64String(ms.ToArray());
}
```

Recommendations

• Evitar el uso de código obsoleto es esencial para mantener la calidad, la seguridad y la mantenibilidad del programa o sistema.

Low severity vulnerabilities

SEVERITY: Low

Los programadores no deben comentar el código, ya que infla los programas y reduce la legibilidad. El código no utilizado debe eliminarse y se puede recuperar del historial de control de código fuente si es necesario. Yo considero que esto puede ser tomado como un falso positivo.

Evidencia:

4.

Solución:

```
{
    Console.WriteLine("Numero de tarjeta invalido!");
}

// Sha256 - Hexadecimal
string vsha256 = Obtenersha256(numeroTarjeta);

// Generamos una clave y un iv (Vector de Inicializacion)
byte[] clave = Generarclave();
byte[] iv = GenerarIV();

// Encriptar
string tarjetaEncriptada = EncriptarAEs(numeroTarjeta, clave, iv);

// Desencriptar
string tarjetaDesencriptada = DesencriptarAEs(tarjetaEncriptada, clave, iv);
```

Recommendations

• Tener código comentado dentro de tu programa es código que no se utiliza por lo tanto lo recomendable sería eliminarlo, ya que esto ayuda a que el tamaño del código no incremente más de lo necesario y su lectura sea más clara.

MICROSOFT TREAT

Threat Modeling Report

Created on 12/21/2023 8:00:44 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

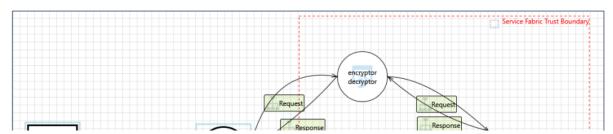
Assumptions:

External Dependencies:

Threat Model Summary:

Not Started 156
Not Applicable 0
Needs Investigation 0
Mitigation Implemented 0
Total 156
Total Migrated 0

Diagram: Diagram 1



MITRE ATT&CK

Fueron seleccionado los grupos de amanezas FIN5, FIN6 y CARBANAK.

FIN5: es un grupo de amenazas motivado financieramente que se ha dirigido a la información de identificación personal y a la información de las tarjetas de pago.

FIN6: es un grupo de ciberdelincuencia que ha robado datos de tarjetas de pago y los ha vendido con fines de lucro en mercados clandestinos.

CARBANAK: es un grupo de ciberdelincuentes que ha utilizado el malware Carbanak para atacar instituciones financieras desde al menos 2013.

Estos grupos fueron seleccionados con su relación a ataques financieros que va relacionado un con el proyecto realizado para el entregable 2. Ya que en nuestro proyecto obtenemos información de la tarjeta de crédito por lo que estos grupos podrían ser una ameneza.

Tecnica:

Valid accounts: La superposición de credenciales y permisos en una red de sistemas es motivo de preocupación porque el adversario puede ser capaz de pivotar entre cuentas y sistemas para alcanzar un alto nivel de acceso.

Mitigación:

Políticas de contraseñas: Las aplicaciones y los dispositivos que utilizan el nombre de usuario y la contraseña predeterminados deben cambiarse inmediatamente después de la instalación y antes de la implementación en un entorno de producción.

Gestión de cuentas de usuario: Asegúrese de que los usuarios y los grupos de usuarios tengan los permisos adecuados para sus roles.

Reporte ATT&CK

Enterprise ATT&CK v14

platforms-

Linux, macOS, Windows, Network, PRE, Containers, Office 365, SaaS, Google Workspace, laaS, Azure AD

legend 1.0 2.0 3.0 4.0 5.0 6.0

Reconnaissance										$\overline{}$			
	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scarring	Acquire Access	Content Bijection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	AdvenayintheMode	Account Discovery	Exploitation of Remote Services	Adversary in the Middle	Application Layer Protocol	Automated Excitosion	Access Removal
ather Victim loc Information	Acquire Infrastructure	Drive-by Comprovise	Command and Scripting Insepretor	BITS Jobs	Access Token Manipulation	Access Token Menipulation	Sinate Force	Application Window Discovery	Internal Speaghtehing	Alchive Collected Data	Communication Through Removable Media	Data Transfer Size Links	Data Destruction
iather Victim lentily Information	Companies Accounts	Exploit Public-Facing Application	Container Administration-Command	SectorLogon Autostat Execution	Account Manipulation	BITS John	Credentals fore Password Stores	Browser Information Discovery	Lateral Tool Tonester	AudoCaptum	Content Injection	Extitation Over Attenutive Protocol	Data Encrypted for impact
lather Victim letwork Information	Componise Infoatucture	External Remote Services	Deploy Container	Sector Legan Initialization Scripts	Boot or Logon Automat Execution	Build Image on Host	Exploitation for Credential Access	Cloud inflattucture Discovery	Remote Service Session Hijacking	Automated Collection	Data Encoding	Extitution OverC2/Channel	Data Manipulation
Sether Victim Organismation	Develop Capabilities	Hardwan Additions	Exploitation for Client Execution	Browser Extensions	Stoot or Logan Initialization Scripts	Debugger Evenion	Foxed Authorization	Cloud Service Dashboard	Remote Services	Browser Session Hilacking	Data Obtained	Extitution Over Other Network Medium	Defacement
Mishing for Monution	Exterior Accounts	Phinting	InterProcess Communication	Componise Client Software Binary	Create or Modify System Process	DeathuscateDecode Rise or information	Fage Web Credentials	CloudService Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution	Extitution Over Physical Medium	DiskWipe
learth Cosed Sources	Cessin Cassibilities	Replication Though Removable Media	NativeAPI	Create Account	Domain Policy Modification	Deploy Container	InstCaste	CloudStoage Object Discovery	Softwan Deployment Tools	Datafore Cloud Storage	Encrypted Channel	Excitation OverWeb Service	Endpoint Denial of Senice
earch Open schrical Databases	Stage	Supply Chain	Scheduled	Create or bladly	Escape to Host	Direct Volume Access	Modify Authentication Process	Container and Resource Discovery	Take Shared Context	Data from Configuration Repository	Falback	Scheduled Transfer	Financial
learth Open	Capabilities	Compranies Trusted	Task/Job Servetess	System Piccess Event Tiggend	Evert Tiggend	Domain Policy	Multi-Factor AutherEcution	Debugger	Use Alternate Authorisation Modelal	Data fore information	Channels Ingress Tool Toursler	Transfer Data	Twt
Nobelber/Domains earth Victim-Owned	1	Relationship Valid Accounts	Shand Mobiles	Execution Execution	Execution Exploitation for	Middlession Execution	Interception Multi-Factor Authentication	Evasion Device Driver	Montal	Repositories Data fore	Mus-Gage	to-Cloud-Account	Comption Inhibit System
Videbis	J	Vaid Accounts	Software	Remate Services Hijack	Privilege Escalation Hijack	Guerdalis Exploitation for	Request Generation	Discovery Dorsein Trust	-	Local System Data fore Network	Channels Non-Application		Recovery Network Denial
			Deployment Tools System	Execution/Row Implant	Execution Row Process	Defense Evasion Rie and Directory Permissions	Sniffing CS Cedental	Discovery File and Directory	-	SharedDrive Datafore	Layer Protocol Non-Strandard		of Service Resource
			Senices	Internal Image	Irjector	Directory Permissions Middlication	Dumping	Discovery		Renouble Meda	Pot		Hijacking
			User Execution	Modify Authoritication Process	Scheduled Task/Job	HideArthon	Steal Application Access Token	GroupPolicy Discovery		DataStaged	Protocol Tunneling	ļ	Siervice Stop
			Windows Management Instrumentation	Office Application Statup	Valid Accounts	Hijack Execution Flow	Steel or Fage Authentication Certificates	Log Enumention		E-mail Collection	Piney		System Shutdown Reboot
				Power Settings		Impair Defenses	Steal or Forge Kerberon Tickets	Natural Service Discovery		Input Capture	Remain Access Software		
				Pre-CS Boat]	Imperioration	Steal Web Session Cookie	Network Share Discovery]	Screen Capture	Traffic Signaling	1	
				Scheduled TankLisb	1	Indicator Removal	Unsecured Credentals	Network Smilling	1	Video Capture	Web Service	1	
				SeverSchan	1	Indirect Command Execution	Constant	Password Policy	1				
				Component Teaflic	1	Managara	1	Discovery Periphenii	1				
				Signaling Valid Accounts		Modify Authorisation	-	Device Discovery Permission	+				
				Vaid Accounts		Process Middly Cloud Compute	-	Groups Discovery Process	-				
						Infrastructure Modify	-	Discovery	-				
						Registry	-	Query Registry Remain System					
						System/trage		Discovery					
						Network Boundary Bridging		Sohoan Discovery					
						Obfuscated Files or Information		System Information Discovery					
						Plat File Modification	1	System Location Discovery]				
						PiterFile Middifusion Pre-OS Boot]	Discovery System Network Configuration					
						NedS Box Proces		Discovery System Network Configuration Discovery System Network					
						Modification Pre-OS Scot Process Injection Refereive		Discovery System System Network Configuration Discovery System Network Connections Discovery System Owner/liver					
						Madification Pre-OS Boor Process Injection Refactive Code Loading Rogue Donain		Statoway System System Materials Configuration Discovery System Naturals Connections Discovery System Connections Statoway System Sentice					
						Neddication Pre-CG Boot Process Injection Refective Code Loading Rogue Domain Controller		Discovery System Configuration Discovery System Network Configuration Discovery System Connections System Connections System Connections System Service System Service System Service System Service					
						Neudification Pre-OS Book Process Pipicasion Reflective Costs Loading Regue Doralin Controller Regue Transition Controller		Discovery Systems National Configuration Discovery System National Connectional Discovery System Connectional Discovery System Sanica Discovery System Connectional Theory Systems Timus Discovery					
						Redification Process Process Process Spiced on Redenderine Code Loading Repue Consilin Controller Reacted Subset Tatact Controls		Discovery System Configuration Discovery System Network Configuration Discovery System Connections System Connections System Connections System Service System Service System Service System Service					
						Haddication Practife door Prac		Discovery Systems Network Configuration (Stationary Systems Network Commissional Stationary Systems Obscovery Systems Connectionary Systems Genicle Chicanopy Systems Genicle Chicanopy Systems Genicle Chicanopy Systems Familian Time Discovery					
						Medication Prace di acra System System Caste Lacing Repub Derman Galle Lacing Repub Derman Control Galle Lacing Repub Derman Control Galle Lacing Repub Derman Control Galle Derman System State System		Discovery Systems Network Configuration (Stationary Systems Network Commissional Stationary Systems Obscovery Systems Connectionary Systems Genicle Chicanopy Systems Genicle Chicanopy Systems Genicle Chicanopy Systems Familian Time Discovery					
						Haddindon Proc G Bare Proc G B		Discovery Systems Network Configuration (Stationary Systems Network Commissional Stationary Systems Obscovery Systems Connectionary Systems Genicle Chicanopy Systems Genicle Chicanopy Systems Genicle Chicanopy Systems Familian Time Discovery					
						Medication Procisi Seas Igination Influence Contribution Impactor Inguina Ing		Discovery Systems Network Configuration (Stationary Systems Network Commissional Stationary Systems Obscovery Systems Connectionary Systems Genicle Chicanopy Systems Genicle Chicanopy Systems Genicle Chicanopy Systems Familian Time Discovery					
						Medication Procisi Seas Igination Influence Contribution Impactor Inguina Ing		Discovery Systems Network Configuration (Stationary Systems Network Commissional Stationary Systems Obscovery Systems Connectionary Systems Genicle Chicanopy Systems Genicle Chicanopy Systems Genicle Chicanopy Systems Familian Time Discovery					
						Held state FINATO Size FINATO		Discovery Systems Network Configuration (Stationary Systems Network Commissional Stationary Systems Obscovery Systems Connectionary Systems Genicle Chicanopy Systems Genicle Chicanopy Systems Genicle Chicanopy Systems Familian Time Discovery					
						Held state FINATO Size FINATO		Discovery Systems Network Configuration (Stationary Systems Network Commissional Stationary Systems Obscovery Systems Connectionary Systems Genicle Chicanopy Systems Genicle Chicanopy Systems Genicle Chicanopy Systems Familian Time Discovery					
						Heldenber Freich Ger F		Discovery Systems Network Configuration (Stationary Systems Network Commissional Stationary Systems Obscovery Systems Connectionary Systems Genicle Chicanopy Systems Genicle Chicanopy Systems Genicle Chicanopy Systems Familian Time Discovery					
						Indication Francis Start Franc		Discovery Systems Network Configuration (Stationary Systems Network Commissional Stationary Systems Obscovery Systems Connectionary Systems Genicle Chicanopy Systems Genicle Chicanopy Systems Genicle Chicanopy Systems Familian Time Discovery					
						Heldunius French Sand French		Discovery Systems Network Configuration (Stationary Systems Network Commissional Stationary Systems Obscovery Systems Connectionary Systems Genicle Chicanopy Systems Genicle Chicanopy Systems Genicle Chicanopy Systems Familian Time Discovery					
						Hedricher FROG Seri French Ser		Discovery Systems Network Configuration (Stationary Systems Network Commissional Stationary Systems Obscovery Systems Connectionary Systems Genicle Chicanopy Systems Genicle Chicanopy Systems Genicle Chicanopy Systems Familian Time Discovery					

Summary

Para la realización de esta actividad fue necesario escanear el programa realizado en el entregable 2, el cual se trató implementar un poco de la teoría obtenida durante el curso "Seguridad en Aplicaciones y Mejores Prácticas de Seguridad en Codificación".

En este trabajó se encuentran algunas de las vulnerabilidades encontradas al escanear el programa desarrollado para el segundo entregable. Estas vulnerabilidades estarán organizadas por los niveles Críticos, Altos, Medios y Bajos. También se agregaron algunos falsos positivos.

Lo agregado en este documento fue obtenido del análisis realizado en SonarQube del proyecto.

También se agregó lo realizado con las herramientas MICROSOFT THREAT MODELLING y MITRE ATT&CK, para complementar la información de este entregable.

Security risk matrix

Risk Matrix	Qty
Critical	
High	
Medium	
Low	