


Nro. Alerta:	EC-2022-01	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ALERTA DE SEGURIDAD	 <p>CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT</p>
TLP:	 <p>TLP:BLANCO</p>		
Fecha:	01/01/2022	Error de Microsoft Exchange interrumpe la entrega de correo electrónico	Versión: 1.0

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Sistemas y/o software Abierto
Nivel de riesgo: Medio

II. ALERTA

En diferentes sitios Web se reporta un posible error en el motor de análisis antispam y antimalware; mejor conocido como motor FIP-FS de Microsoft Exchange, provocando que los usuarios no puedan enviar y recibir correos electrónicos.



Figura 1.- Ilustraciones relacionadas a Microsoft Exchange
Fuente: Microsoft

III. INTRODUCCIÓN


Exchange Server 2016 y Exchange Server 2019 emplean una variable INT32 para el registro de fecha siendo el formato empleado: ["YYMMDDHHMM"], para esta variable su rango dinámico se encuentra entre: -2147483648 y -2147483648 o de otra manera ["-2^32 a -2^32].

Estos valores no presentaban inconvenientes para las fechas del 2021; sin embargo, para fechas del actual año, este rango dinámico resulta insuficiente; ya que para el 2022 el valor mínimo de la variable INT32 es 2201010001 y como se puede observar, el valor máximo de INT32 es menor al requerido.

IV. VECTOR DE ATAQUE:

El vector de ataque es local y se espera que la compañía confirme los detalles técnicos.

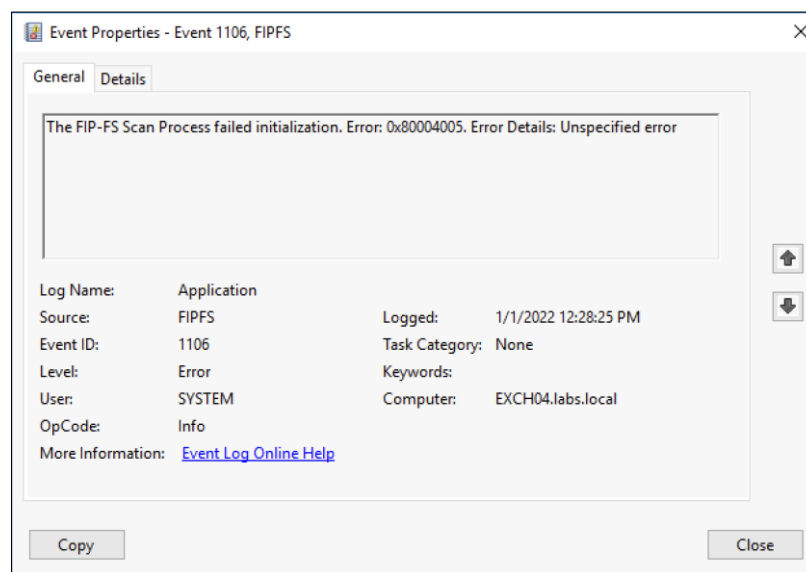


Nro. Alerta:	EC-2022-01	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ALERTA DE SEGURIDAD	 CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	 TLP: BLANCO		
Fecha:	01/01/2022	Error de Microsoft Exchange interrumpe la entrega de correo electrónico	Versión: 1.0

V. IMPACTO:

Este desbordamiento provoca que el motor de escaneo falle y se atasquen las colas de transporte para la entrega del correo. Así mismo, si existe una gran cantidad de correos en cola, el almacenamiento del servidor puede llegar a su límite provocando errores de funcionamiento y un posterior bloqueo.

Adicional a la cola de correo, también se identifica “**EventID 1106**” en el registro de eventos de la aplicación que indica “*The FIP-FS Scan Process failed initialization. Error: 0x80004005. Error Details: Unspecified error*” En la siguiente gráfica, se indica imagen asociada a este error.



```

Machine: EXCH01.labs.local
[PS] C:\Users\administrator.LABS>Get-ExchangeServer | ?{($_.Name -like "EXCH*")} | Get-TransportService | get-queue

Identity           DeliveryType      Status  MessageCount  Velocity  RiskLevel  OutboundIPPool  NextHopDomain
-----
EXCH04\Submission  Undefined         Ready   234           -8        Normal    0                Submission
EXCH02\Submission  Undefined         Ready   0              0        Normal    0                Submission
EXCH02\Shadow\6   ShadowRedundancy Ready   2              0        Normal    0                exch01.labs.local
EXCH01\Submission  Undefined         Ready   3              0        Normal    0                Submission
EXCH12\Submission  Undefined         Ready   2              0        Normal    0                Submission
EXCH12\Shadow\4   ShadowRedundancy Ready   1              0        Normal    0                exch11.labs.local
EXCH11\Submission  Undefined         Ready   1              0        Normal    0                Submission
EXCH11\Shadow\40  ShadowRedundancy Ready   2              0        Normal    0                exch12.labs.local
  
```

Figura 2.- Ilustraciones relacionadas a EventID1106
Fuente: Jaap Wesseliuis

Nro. Alerta:	EC-2022-01	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ALERTA DE SEGURIDAD	 CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	 TLP: BLANCO		
Fecha:	01/01/2022	Error de Microsoft Exchange interrumpe la entrega de correo electrónico	Versión: 1.0

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Mientras Microsoft realiza actualización de Exchange Server se sugiere para los servidores Exchange 2016 y 2019, que se encuentren afectados; [bajo plena responsabilidad de cada uno de los administradores] deshabilitarⁱ el motor de análisis FIP-FS para permitir el envío de correo electrónico. En el siguiente link podrá encontrar más información: <https://docs.microsoft.com/en-us/Exchange/antispam-and-antimalware/antimalware-protection/antimalware-protection?view=exchserver-2019>

VII. REFERENCIAS:

- Abrams, L. (01 de 01 de 2022). *BleepingComputer*. Obtenido de BleepingComputer: <https://www.bleepingcomputer.com/news/microsoft/microsoft-exchange-year-2022-bug-in-fip-fs-breaks-email-delivery/>
- Microsoft. (30 de 11 de 2021). *Microsoft*. Obtenido de <https://docs.microsoft.com/es-es/cpp/cpp/integer-limits?view=msvc-170>
- Microsoft. (s.f.). *Microsoft*. Obtenido de <https://www.microsoft.com/es-ww/microsoft-365/exchange/email>
- microsoft, T. (01 de 01 de 2022). *Blog del equipo de Exchange*. Obtenido de <https://techcommunity.microsoft.com/t5/exchange-team-blog/email-stuck-in-transport-queues/ba-p/3049447>
- Wesselius, J. (01 de 01 de 2022). <https://jaapwesselius.com>. Obtenido de <https://jaapwesselius.com>: <https://jaapwesselius.com/2022/01/01/the-fip-fs-scan-process-failed-initialisation-mail-is-queued-on-exchange-servers/>

ⁱ Preste mucha atención al momento de deshabilitar el motor de análisis; ya que no se analizará el correo entregado, lo que generará más correos electrónicos maliciosos y spam que lleguen a los usuarios