MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

COLCERT

Identificador
[colCERT AL-0930-019]

30/09/2022

Alerta de Seguridad Digital

[TLP: WHITE]

Vulnerabilidades Servidores Exchange

Vulnerabilidades zero-day en Microsoft Exchange

Se ha detectado dos vulnerabilidades zero-day catalogadas como CVE-2022-41040 y CVE-2022-41082, que afectan a Microsoft Exchange Server 2013, 2016 y 2019, Microsoft les ha otorgado una severidad **CRÍTICA**

Las solicitudes utilizadas en esta cadena de explotación son similares a las utilizadas en los ataques dirigidos a las vulnerabilidades de ProxyShell, por lo que se las conoce como ProxyNotShell.

La vulnerabilidad CVE-2022-41040 es de tipo *Server Side Request Forgery* (SSRF), mientras que la segunda, identificada como CVE-2022-41082 permite la ejecución remota de código (RCE). Para que la explotación sea exitosa es necesario disponer de credenciales válidas para el acceso al servidor Exchange vulnerable.

Recursos afectados

Microsoft Exchange Server versiones: 2013, 2016 y 2019.

Solución a las vulnerabilidades

Microsoft ha publicado una Guía donde indica que bloquear los puertos remotos de PowerShell (HTTP: 5985 y HTTPS: 5986) puede limitar la explotación de la vulnerabilidad. También indica una posible mitigación, consistente en agregar una regla de bloqueo para bloquear los patrones de ataque conocidos.

Recomendaciones

Aplicar las medidas contempladas en la “Guía para el cliente sobre vulnerabilidades de día cero notificadas en Microsoft Exchange Server” de manera urgente.

Lo anterior según lo señalado por el CCN CERT en su alerta https://www.ccn-cert.cni.es/seguridad-al-dia/alertas-ccn-cert/12060-vulnerabilidades-zero-day-en-microsoft-exchange.html

ProxyShell de Microsoft Exhange Server SSRF - CVE-2021-34473

Teniendo en cuenta la filtración de información principalmente de correos electrónicos, realizado por el grupo ambientalista Guacamaya, de algunas entidades de gobierno de algunos países incluido entre ellos Colombia, publicado el 19 de septiembre del 2022, en el sitio web (https://ddosecrets.com/wiki/Distributed_Denial_of_Secrets),

Se ha podido determinar con base en la información disponible y compartida al COLCERT, que este grupo viene explotando vulnerabilidades como la del CVE-2021-34473, denominada ProxyShell de Microsoft Exhange Server SSRF y las relacionados los CVE-2021-34523 y CVE-2021-31207.

Contexto

ProxyShell, es una combinación de 3 vulnerabilidades CVE-2021-34473, CVE-2021-34523 y CVE-2021-31207 que juntas se utilizan para la ejecución remota de código y la escalada de privilegios, es una vulnerabilidad de falsificación de solicitudes del lado del servidor (SSRF), donde un atacante puede realizar solicitudes a recursos internos del servidor, sin necesidad de autenticación en su nombre. La vulnerabilidad se produce debido a un problema de confusión de ruta de acceso en el que el URI (siglas de *uniform resource identifier* o identificador uniforme de recursos) se analiza incorrectamente.

Proxy shell se confunde con proxylogon. El inicio de sesión de proxy fue utilizado por un famoso actor de amenazas "Hafnium" en marzo de 21 para atacar múltiples exchange server. Las vulnerabilidades asociadas con ambos son diferentes. En el inicio de sesión de proxy, las 2 vulnerabilidades asociadas fueron CVE-2021-26855 (vulnerabilidad de omisión de autenticación de Exchange Server) y CVE-2021-27065 (vulnerabilidad de escritura de archivo arbitrario posterior a la autenticación).

Dado que proxyshell es una combinación de 3 vulnerabilidades, al explotarlo se realizaría una fuga masiva de datos e información.
La vulnerabilidad existe en el exchange server on premise que se usa masivamente incluso ahora en la era de la nube. Teniendo en cuenta que los exchange server están de cara a Internet, la superficie de ataque es fácilmente accesible para un atacante.

CVE-2021-34473:

Esta es una vulnerabilidad de ejecución remota de código de Microsoft Exchange, existe una falla en el servicio de detección automática originada de una validación incorrecta del URI antes de acceder a los recursos. Un atacante puede usar esto junto con otras vulnerabilidades para ejecutar código arbitrario en el contexto del "Sistema" del usuario que generalmente tiene acceso de administrador.

CVE-2021-34523:

Esta es otra vulnerabilidad de ejecución remota de código de Microsoft Exchange en la que la validación del token de acceso antes de PowerShell es incorrecta. Con esta se puede obtener acceso de usuario del "Sistema" que a su vez tiene acceso de administrador.

CVE-2021-31207:

La vulnerabilidad existe debido a una falla en el manejo de la exportación de buzones. El cual ocurre debido a la falta de una validación adecuada de los datos proporcionados por el usuario y el cargue de archivos arbitrarios. Un atacante puede usar esta falla para obtener acceso con privilegios de nivel de "Sistema".

Ciclo de vida del soporte de Microsoft Exchange Server.

Exchange Server 2013
https://learn.microsoft.com/es-es/lifecycle/products/exchange-server-2013

Lista	Fecha de inicio	Fecha de finalización estándar	Fecha de finalización ampliada
Exchange Server 2013	9 ene 2013	10 abr 2018	11 abr 2023

Version	Fecha de inicio	Fecha de finalización
Service Pack 1	25 feb 2014	11 abr 2023
Original Release	9 ene 2013	14 abr 2015

Exchange Server 2016
https://learn.microsoft.com/es-es/lifecycle/products/exchange-server-2016

Lista	Fecha de inicio	Fecha de finalización estándar	Fecha de finalización ampliada
Exchange Server 2016	1 oct 2015	13 oct 2020	14 oct 2025

Exchange Server 2019
https://learn.microsoft.com/es-es/lifecycle/products/exchange-server-2019

Lista	Fecha de inicio	Fecha de finalización estándar	Fecha de finalización ampliada
Exchange Server 2019	22 oct 2018	9 ene 2024	14 oct 2025

Recomendaciones:

Las entidades con servidores *On Premise* sin parchear realzar las siguientes actividades de mitigación:

1. Seguir las instrucciones de Microsoft para determinar el compromiso:

https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/
https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/

Si no se ha identificado ningún compromiso, siga las siguientes recomendaciones de parches

a. Microsoft ha indicado que las siguientes versiones y actualizaciones acumulativas (CU) de Exchange deben instalarse antes de la actualización de seguridad.
b. Exchange Server 2010 (la actualización requiere SP 3 o cualquier RU de SP 3)
c. Exchange Server 2013 (la actualización requiere CU 23)
d. Exchange Server 2016 (la actualización requiere CU 19 o CU 18)
e. Exchange Server 2019 (la actualización requiere CU 8 o CU 7)

Actualización de seguridad para Exchange Server 2019 CU9 (KB5001779): https://www.microsoft.com/en-us/download/details.aspx?id=103004

Actualización de seguridad para Exchange Server 2013 CU23 (KB5001779): https://www.microsoft.com/en-us/download/details.aspx?id=103000

Actualización de seguridad para Exchange Server 2019 CU8 (KB5001779): https://www.microsoft.com/en-us/download/details.aspx?id=103003

Actualización de seguridad para Exchange Server 2016 CU19 (KB5001779): https://www.microsoft.com/en-us/download/details.aspx?id=103001

Actualización de seguridad para Exchange Server 2016 CU20 (KB5001779): https://www.microsoft.com/en-us/download/details.aspx?id=103002

Nota: Todas las actualizaciones (CU y la actualización de seguridad) deben ejecutarse como administrador y Microsoft ha notado que es posible que se requieran varios reinicios. Información adicional sobre la aplicación de parches está disponible a través del blog de la comunidad tecnológica de Microsoft.

3. Continuar revisando las páginas informativas de Microsoft respecto de actualizaciones y recomendaciones para proteger mejor su infraestructura, sistemas y posibles opciones de respuesta ante compromisos.
4. De ser posible migrar los sistemas de correo electrónico de Exchange local a Exchange Online, a todas las entidades de orden nacional y territorial, lo anterior teniendo en cuenta este set de vulnerabilidades.
5. Validar el servicio de TELNET, si este se encuentra habilitado hacia el servidor de correo desde redes externa e internas.
6. Bloquear el acceso a los servidores de correo a través de “telnet”, para evitar el envió de correo por la línea de comando.

Referencias:

https://www.ccn-cert.cni.es/seguridad-al-dia/alertas-ccn-cert/12060-vulnerabilidades-zero-day-en-microsoft-exchange.html
https://www.techtarget.com/whatis/feature/Everything-you-need-to-know-about-ProxyShell-vulnerabilities

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41040
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41082
https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34473
https://learn.microsoft.com/es-es/exchange/use-telnet-to-test-smtp-communication-exchange-2013-help

Canales de Atención

Si tiene alguna consulta técnica, puede comunicarse con CSIRT Gobierno de tratarse de una entidad del Estado, o con COLCERT si pertenece a cualquier otro sector de la economía, a través de los siguientes canales:

Bogotá: +57 601 344 22 22
Línea Gratuita Nacional: 018000952525 Opción 2

contacto@colcert.gov.co,
csirtgob@mintic.gov.co

@colCERT