USTIC-ALERT 03/22. Vulnerabilidades “día cero” en Microsoft Exchange Server (03/10/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones, siguiendo las indicaciones marcadas por el CCN-CERT, del Centro Criptológico Nacional, **alerta de la publicación de dos vulnerabilidades de “día cero” que afectan a Microsoft Exchange Server 2013, 2016 y 2019 que podrían permitir a un ciberatacante ejecutar código de forma remota.**

Detalle

Microsoft está investigando dos vulnerabilidades de día cero, calificadas por la compañía como críticas, que afectan a Microsoft Exchange Server 2013, Exchange Server 2016 y Exchange Server 2019. La primera, identificada como CVE-2022-41040, es una vulnerabilidad de falsificación de solicitud del lado del servidor (SSRF) y, la segunda, identificada como CVE-2022-41082, permite la ejecución remota de código (RCE) cuando PowerShell es accesible para el atacante.

De acuerdo con la información publicada, **estas vulnerabilidades están siendo explotada activamente por atacantes remotos**, lo que se traduce en un escenario de riesgo, por lo que se ruega se sea especialmente diligente en su resolución. Llamamos vuestra atención sobre la urgencia de aplicar las recomendaciones indicadas y la adopción de medidas para hacer frente a las vulnerabilidades.

Sistemas Afectados

- Exchange Server 2013;
- Exchange Server 2016;
- Exchange Server 2019.

Recomendaciones Actualizadas (03/10/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones recomienda encarecidamente aplicar los siguientes pasos, con el fin de evitar la exposición a ataques externos y la toma de control de los sistemas:

Mitigación

1º. Solución a las vulnerabilidades:

En estos momentos **no hay disponible una actualización o parche de seguridad** que corrija estas vulnerabilidades. Asimismo, indican desde Microsoft que los clientes de Exchange Online no necesitan realizar ninguna acción porque la empresa cuenta con sistemas de detección y mitigación para protegerlos. Mientras tanto, la organización recomienda aplicar una serie de medidas de mitigación, que serán resumidas a continuación.

2º. *Workaround* de las vulnerabilidades:

- Deshabilitar el acceso remito a PowerShell para los usuarios que no sean administradores de la organización.
- Bloquear los puertos remotos de PowerShell (HTTP: 5985 y HTTPS: 5986) expuestos también puede limitar la explotación.
- Agregar una regla de bloqueo en "*IIS Manager -> Default Web Site -> URL Rewrite -> Actions*" para bloquear los patrones de ataque conocidos, tal como se detalla **aquí**.

Referencias

- Alerta CCN-CERT Exchange
- Customer Guidance for Reported Zero-day Vulnerabilities in Microsoft Exchange Server – Microsoft Security Response Center
- Warning: New attack campaign utilized a new 0-day RCE vulnerability on Microsoft Exchange Server | Blog | GTSC - Cung cp các dch v bo mt toàn din (gteltsc.vn)
- ProxyNotShell— the story of the claimed zero days in Microsoft Exchange | by Kevin Beaumont | Sep, 2022 | DoublePulsar
- Suspected Post-Authentication Zero-Day Vulnerabilities in Microsoft Exchange Server | Rapid7 Blog
- SECURITY ALERT: Attack Campaign Utilizing Microsoft Exchange 0-Day (trendmicro.com)

En caso de haber detectado la explotación de esta vulnerabilidad :

debe reportar el incidente mediante correo electrónico a sau.cges.sspa@juntadeandalucia.es indic ando en el *Asunto: [Compromiso Exchange1022]*

Para cualquier otra duda o consulta al respecto, puede ponerse en contacto con ustic.stic.sspa@juntadeandalucia.es.

Gracias por vuestra atención.

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud