BEACON LAB

C S I R T

CYBOLT

Security Innovation

Boletín de Alerta

Boletín Nro.: 2023-07
Fecha de publicación: 6/11/2023
Tema: PoC publicó para vulnerabilidad RCE critica de Microsoft Exchange Server
Traffic Light Protocol (TLP): White

Producto afectado:

- Microsoft Exchange Server 2016 Cumulative Update 23
- Microsoft Exchange Server 2019 Cumulative Update 12
- Microsoft Exchange Server 2019 Cumulative Update 13

Descripción:

Se ha reportado una vulnerabilidad critica que afecta al Servidor de Correo Microsoft Exchange Server denominada CVE-2023-36745 clasificada como Alta con un puntaje de CVSS de 8.0, que puede permitir a atacantes remotos ejecutar código remoto (RCE).

Esta vulnerabilidad se aprovecha aprovechando la clase Microsoft.Exchange.DxStore.Common.DxSerializationUtil.SharedTypeResolver para evadir las restricciones de seguridad predeterminadas de .NET Framework. Esta clase se puede emplear para cargar ensamblados (assemblies) desde ubicaciones remotas, lo que posteriormente permite la ejecución de código arbitrario en el sistema de la víctima.

Un atacante podría aprovechar la vulnerabilidad aprovechando el gadget (Tipo 4) UnitySerializationHolder mediante una deserialización de datos que no son de confianza. La explotación de esta vulnerabilidad requiere que el atacante obtenga acceso a la LAN y obtenga credenciales para un usuario válido de Exchange.

Se ha publicado un exploit de Prueba de Concepto (PoC) para la vulnerabilidad CVE-2023-36745 de Microsoft Exchange Server, se recomienda tomar medidas correctivas inmediatamente.

Adicionalmente, se han corregido otras 3 vulnerabilides, CVE-2023-36756, CVE-2023-36757 y CVE-2023-36744 todas con un puntaje de CVSS de 8.0 con criticidad Alta y CVE-2023-36777 ya con un puntaje de 5.7 y criticidad media.

Es posible que los atacantes aprovechen algunas de estas vulnerabilidades como parte de una estrategia de movimiento lateral durante un ataque, pudiendo exfiltrar información sensible, entre otras acciones.

Investigadores independientes han afirmado haber encontrado adicionalmente otras 4 vulnerabilidades (ZDI-23-1578, ZDI-23-1579, ZDI-23-1580 y ZDI-23-1581), las cuales hasta el momento no tienen parche, sin embargo, de acuerdo a declaraciones de representantes de Microsoft, no hay evidencia de que sean explotables desde fuera de la red, además de requerir también autentitcación. Estas vulnerabilidades todavía no han sido incluidas para su corrección y serán abordadas en parches futuros

Impacto:

- Puede conducir a un ataque que previamente hubiera conseguido acceso a la red, tomar el control total del servidor Exchange y conseguir información sensible de toda la organización
- Una explotación exitosa también podría causar un tiempo de inactividad en el sistema objetivo.

Solución:

Se recomienda encarecidamente a los administradores que instalen y apliquen parches a las últimas actualizaciones de seguridad de MS Exchange Server para evitar posibles violaciones de seguridad.

Guía de seguridad oficial para abordar el CVE-2023-36745

https://support.microsoft.com/en-us/topic/description-of-version-2-of-the-security-update-for-microsoft-exchange-server-2019-and-2016-august-15-2023-kb5030524-940cdc34-07c4-441e-b0f4-c5a19779d715

Actualizaciones

- Microsoft Exchange Server 2016 Cumulative Update 23
  https://www.microsoft.com/en-us/download/details.aspx?id=105536
- Microsoft Exchange Server 2019 Cumulative Update 12
  https://www.microsoft.com/en-us/download/details.aspx?id=105535
- Microsoft Exchange Server 2019 Cumulative Update 13
  https://www.microsoft.com/en-us/download/details.aspx?id=105534

También se recomienda a los administradores instalar Exchange Server Health Checker (https://microsoft.github.io/CSS-Exchange/Diagnostics/HealthChecker/) para detectar problemas de configuración comunes que se sabe que causan problemas de rendimiento y otros problemas de larga duración que son causado por un simple cambio de configuración dentro de un entorno Exchange.

Información adicional:

- https://securityonline.info/microsoft-exchange-server-rce-cve-2023-36745-flaw-gets-poc-exploit/
- https://techcommunity.microsoft.com/t5/exchange-team-blog/september- 2023-lanzamiento-del-nuevo-servidor-exchange-cves-resolved-by/ba-p/3924063
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36745
- https://vulnera. com/newswire/microsoft-exchange-server-vulnerability-poc-exploit-for-cve-2023-36745-published/
- https://nvd.nist.gov/vuln/detail/CVE-2023-36745

CYBOLT
Security Innovation

BEACON LAB

C S I R T

contact@cybolt.com

cybolt.com