Nro. Alerta:	EC-2022-090	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:CLEAR		
Fecha:	30-sept-2022	MÚLTIPLES VULNERABILIDADES EN MICROSOFT EXCHANGE SERVER	V 1.1

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de vulnerabilidad: CVE-2022-41040 / CVE-2022-41082
Nivel de riesgo: Varios niveles de impacto.

II. ALERTA

Múltiples vulnerabilidades en Microsoft Exchange Server podrían permitir ataques remotos y ejecución de código malicioso.

Las vulnerabilidades detectadas han sido registradas en los sistemas de métricas de priorización con los registros CVE-2022-41040 y CVE-2020-41082, que señalan como tecnicass de ataque utilizadas, Server-Side Request Forgery y Remote Code Execution.

Figura No. 1: Vulnerabilidades Microsoft Exchange Server

III. INTRODUCCIÓN

Microsoft Exchange Server es una aplicación para servidor de correo utilizada por organizaciones a fin de proveer y gestionar el servicio de correo electrónico. Las vulnerabilidades detectadas permitirán el comprometimiento de las credenciales de una determinada de cuenta de usuario, y a través de la misma en función de su nivel de privilegios, se podría instalar programas, modificar activos de información, crear nuevas cuentas de usuarios con fines maliciosos.

Dirección: Av. 9 de Octubre N27-75 y Berlín
Código Postal: 170513 / Quito - Ecuador
Teléfono: 593-2 2946 400 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-090	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:CLEAR		
Fecha:	30-sept-2022	MÚLTIPLES VULNERABILIDADES EN MICROSOFT EXCHANGE SERVER	V 1.1

Las vulnerabilidades detectadas afectan a las versiones:

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

IV. VECTOR DE ATAQUE: Explotación de servicios remotos

V. IMPACTO:

En consideración al tipo de arquitectura y alcance de la red en la que se encuentre se han definido los siguientes tipos de impacto:

- Redes Institucionales de gran alcance: Alto
- Redes Institucionales de bajo alcance: Medio
- Redes de Hogar: Bajo

VI. INDICADORES DE COMPROMISO:

No aplica.

VII. RECOMENDACIONES:

El Centro de Respuestas a Incidentes Informáticos de ARCOTEL, EcuCERT, recomienda a su comunidad objetivo y a la ciudadanía lo siguiente:

- Aplicar los parches de seguridad y procedimientos mitigatorios definidos por el desarrollador de la aplicación.
- Verificar el proceso de actualización automática de la herramienta.
- Verificar el principio de menor privilegio respecto de la gestión de cuentas de usuarios.

VIII. ACTUALIZACIÓN (06-octubre-2022)

Investigadores han detectado que las medidas de mitigación inicialmente emitidas Microsoft, tendrían limitaciones respecto del espectro de ataques que podrían explotar las vulnerabilidades CVE-2022-41040 y CVE-2020-41082 y en consideración a las

Dirección: Av. 9 de Octubre N27-75 y Berlín
Código Postal: 170513 / Quito - Ecuador
Teléfono: 593-2 2946 400 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-090	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:CLEAR		
Fecha:	30-sept-2022	MÚLTIPLES VULNERABILIDADES EN MICROSOFT EXCHANGE SERVER	V 1.1

pruebas de concepto generadas, Microsoft ha emitido una actualización a las acciones de mitigación a fin de que los administradores de la aplicación puedan considerarlas para aplicación de acuerdo a su entorno particular.

IX. DESCARGO DE RESPONSABILIDAD

- La información en esta alerta es con fines informativos. El Centro de Respuestas de ARCOTEL, EcuCERT, no respalda ningún producto o servicio comercial, incluidos aquellos sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante, no constituye ni implica respaldo, recomendación o favorecimiento por parte de EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

X. REFERENCIAS:

- *Microsoft Security Response Center. (2022, 29 septiembre). Customer Guidance for Reported Zero-day Vulnerabilities in Microsoft Exchange Server. Recuperado de https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/*
- *CISA. (2022, 30 septiembre). Microsoft Releases Guidance on Zero-Day Vulnerabilities in Microsoft Exchange Server. Recuperado de https://www.cisa.gov/uscert/ncas/current-activity/2022/09/30/microsoft-releases-guidance-zero-day-vulnerabilities-microsoft*
- *Condon, C. (2022, 30 septiembre). CVE-2022-41040 and CVE-2022-41082: Unpatched Zero-Day Vulnerabilities in Microsoft Exchange Server. Recuperado de https://www.rapid7.com/blog/post/2022/09/29/suspected-post-authentication-zero-day-vulnerabilities-in-microsoft-exchange-server/*
- *Ilasucu, I. (2022, 03 octubre). Microsoft Exchange Server Zero-Day mitigation can be bypassed. Recuperado de https://www.bleepingcomputer.com/news/security/microsoft-exchange-server-zero-day-mitigation-can-be-bypassed/*

Nro. Alerta:	EC-2022-090	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:CLEAR		
Fecha:	30-sept-2022	MÚLTIPLES VULNERABILIDADES EN MICROSOFT EXCHANGE SERVER	V 1.1

Dirección: Av. 9 de Octubre N27-75 y Berlín
Código Postal: 170513 / Quito - Ecuador
Teléfono: 593-2 2946 400 - www.arcotel.gob.ec