# BOLETÍN DE ALERTA

**Boletín Nro.**: 2021-27

**Fecha de publicación**: 24/09/2021

**Tema**: Fuga de credenciales debido a errores de detección automática de Microsoft Exchange.

**Productos afectados:**

- Microsoft Exchange.

**Descripción:**

Especialistas en ciberseguridad han reportado la detección de un error de diseño en una función del servidor email de **Microsoft Exchange** que podría ser abusado por actores de amenazas con el fin de recolectar dominios **Windows** y credenciales de aplicaciones de los usuarios.

Los investigadores mencionan que el error reside en el protocolo **Microsoft Autodiscover**, una característica de los **servidores email** en Exchange que permite a los clientes de email detectar automáticamente un servidor, proporcionar credenciales y recibir las configuraciones correspondientes.

Este protocolo es un elemento fundamental para los servidores email de Exchange, pues permite a los administradores asegurarse de que los clientes usen configuraciones como SMTP, IMAP, LDAP y WebDAV, entre otras. Acceder a estas configuraciones automáticas permitiría a los clientes email hacer ping a un conjunto de URLs predeterminadas, todas derivadas del dominio email del usuario:

- https://autodiscover.example.com/autodiscover/autodiscover.xml
- http://autodiscover.example.com/autodiscover/autodiscover.xml
- https://example.com/autodiscover/autodiscover.xml
- http://example.com/autodiscover/autodiscover.xml

Este mecanismo de detección automática utilizaba un procedimiento back-off en caso de no encontrar el endpoint del servidor Exchange en un primer intento: Este mecanismo es la causa de la filtración porque siempre intenta resolver la parte de detección automática del dominio y siempre intentará fallar. El resultado del próximo intento de crear una URL de detección automática sería: http://autodiscover.com/autodiscover/autodiscover.xml, lo que significa que el propietario de autodiscover.com recibirá todas las solicitudes que no puedan llegar al dominio original.

**Impacto:**

Si un atacante controla los dominios de detección automática de nivel superior (o si el atacante tiene la capacidad de realizar un ataque de envenenamiento DNS utilizando estos dominios), puede obtener muy fácilmente las credenciales de dominio válidas de estas solicitudes de Autodiscover con fugas.

**Mitigación:**

La mitigación de este problema requieren acciones tanto por parte de los administradores de tecnologías basadas en intercambio como Outlook o ActiveSync (protocolo de sincronización de intercambio móvil de Microsoft); así como también acciones por parte de desarrolladores/proveedores de software que están implementando el protocolo de detección automática en sus productos. Se espera que éstos publiquen actualizaciones o parches en algún futuro.

Por parte de los administradores, se recomiendan las siguientes acciones:

- Asegúrese de estar bloqueando activamente los dominios de detección automática. <tld> (como autodiscover.com/autodiscover.com.cn, etc.) en su firewall.
    - Al implementar configuraciones de intercambio, asegúrese de que la compatibilidad con la autenticación básica esté deshabilitada. Usar la autenticación básica HTTP es lo mismo que enviar una contraseña en texto sin cifrar por cable.

- Puede encontrar una lista textual completa de todos los dominios de nivel superior en: https://data.iana.org/TLD/tlds-alpha-by-domain.txt

**Información adicional:**

- https://www.guardicore.com/labs/autodiscovering-the-great-leak/
- https://searchdatacenter.techtarget.com/es/noticias/252507117/Fuga-en-Autodiscover-de-Microsoft-deriva-en-filtracion-de-miles-de-contrasenas
- https://therecord.media/microsoft-exchange-autodiscover-bug-leaks-hundreds-of-thousands-of-domain-credentials/