

# CYBER **SECURITY** **NEWS**

SECURITY OPERATIONS CENTER

**La violación de datos de Microsoft  
expone la información de contacto y los  
correos electrónicos de los clientes.**

*20/Octubre/2022*

## Contenido

Introducción .....	3
Filtración de datos de clientes de Microsoft .....	4
Resumen .....	4
Datos filtrados supuestamente vinculados a 65.000 entidades en todo el mundo.....	5
Herramienta en línea para buscar los datos filtrados .....	6
Recomendaciones.....	8
Noticia Completa .....	8
Enlace a Bluebleed.....	8
Contactos de soporte .....	9

## INTRODUCCIÓN

Microsoft dijo hoy que parte de la información confidencial de sus clientes fue expuesta por un servidor de Microsoft mal configurado accesible a través de Internet.

## FILTRACIÓN DE DATOS DE CLIENTES DE MICROSOFT

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2022_10_20_01
Clasificación de alerta:	Amenaza
Tipo de Impacto:	Alto
TLP (Clasificación de información):	<b>CLEAR</b>
Fecha de publicación:	10/20/2022
Es día cero (0 day):	No

## RESUMEN

La empresa aseguró el servidor después de que los investigadores de seguridad de la empresa de inteligencia de amenazas SOCRadar le notificaran la filtración el 24 de septiembre de 2022.

"Esta mala configuración resultó en el potencial de acceso no autenticado a algunos datos de transacciones comerciales correspondientes a interacciones entre Microsoft y posibles clientes, como la planificación o la posible implementación y provisión de servicios de Microsoft", reveló la compañía .

"Nuestra investigación no encontró indicios de que las cuentas o los sistemas de los clientes estuvieran comprometidos. Notificamos directamente a los clientes afectados".

Según Microsoft, la información expuesta incluye nombres, direcciones de correo electrónico, contenido de correo electrónico, nombre de la empresa y números de teléfono, así como archivos vinculados a negocios entre los clientes afectados y Microsoft o un socio autorizado de Microsoft.

Redmond agregó que la fuga fue causada por la "configuración incorrecta no intencional en un punto final que no está en uso en todo el ecosistema de Microsoft" y no debido a una vulnerabilidad de seguridad.

## DATOS FILTRADOS SUPUESTAMENTE VINCULADOS A 65.000 ENTIDADES EN TODO EL MUNDO

Si bien Microsoft se abstuvo de proporcionar detalles adicionales sobre esta fuga de datos, SOCRadar reveló en una publicación de blog publicada hoy que los datos se almacenaron en Azure Blob Storage mal configurado.

En total, SOCRadar afirma que pudo vincular esta información confidencial a más de 65,000 entidades de 111 países almacenadas en archivos con fecha de 2017 a agosto de 2022.

"El 24 de septiembre de 2022, el módulo de seguridad en la nube integrado de SOCRadar detectó un Azure Blob Storage mal configurado mantenido por Microsoft que contenía datos confidenciales de un proveedor de nube de alto perfil", dijo SOCRadar .

La compañía de inteligencia de amenazas agregó que, a partir de su análisis, los datos filtrados "incluyen documentos de prueba de ejecución (PoE) y declaración de trabajo (SoW), información del usuario, pedidos/ofertas de productos, detalles del proyecto, PII (información de identificación personal) datos y documentos que puedan revelar la propiedad intelectual".

Microsoft agregó hoy que cree que SOCRadar "exageró enormemente el alcance de este problema" y "los números".

Además, Redmond dijo que la decisión de SOCRadar de recopilar los datos y hacer que se puedan buscar mediante un portal de búsqueda dedicado "no es lo mejor para garantizar la privacidad o seguridad del cliente y exponerlos potencialmente a riesgos innecesarios".

Según una alerta del Centro de administración de Microsoft 365 con respecto a esta violación de datos publicada el 4 de octubre de 2022, Microsoft "no puede proporcionar los datos específicos afectados por este problema".

Según los informes , el equipo de soporte de la compañía también les dijo a los clientes que se comunicaron que no notificaría a los reguladores de datos porque "no se requieren otras notificaciones bajo GDPR" además de las enviadas a los clientes afectados.

## HERRAMIENTA EN LÍNEA PARA BUSCAR LOS DATOS FILTRADOS


El portal de búsqueda de fugas de datos de SOCRadar se llama BlueBleed y permite a las empresas averiguar si su información confidencial también estuvo expuesta con los datos filtrados.

Además de lo que se encontró dentro del servidor mal configurado de Microsoft, BlueBleed también permite buscar datos recopilados de otros cinco cubos de almacenamiento público.


Solo en el servidor de Microsoft, SOCRadar afirma haber encontrado 2,4 TB de datos que contienen información confidencial, con más de 335 000 correos electrónicos, 133 000 proyectos y 548 000 usuarios expuestos descubiertos al analizar los archivos filtrados hasta ahora.







Según el análisis de SOCRadar, estos archivos contienen correos electrónicos de clientes, documentos SOW, ofertas de productos, trabajos POC (prueba de concepto), detalles del ecosistema de socios, facturas, detalles del proyecto, lista de precios de productos del cliente, documentos POE, pedidos de productos, documentos firmados del cliente, comentarios internos para clientes, estrategias de ventas y documentos de activos fijos de clientes.

"Los actores de amenazas que pueden haber accedido al depósito pueden usar esta información de diferentes formas para extorsionar, chantajear, crear tácticas de ingeniería social con la ayuda de información expuesta o simplemente vender la información al mejor postor en la web oscura y los canales de Telegram". advirtió SOCRadar.



Find out if your data has been exposed



 6 Buckets  123 Countries  150K Companies  200K Project Files  ~1 Million Emails  800K Users

**PORTAL DE BÚSQUEDA BLUEBLEED**

"No se descargaron datos. Algunos de los datos fueron rastreados por nuestro motor, pero como prometimos a Microsoft, hasta ahora no se han compartido datos, y todos estos datos rastreados se eliminaron de nuestros sistemas"

"Redireccionamos a todos nuestros clientes a MSRC si desean ver los datos originales. La búsqueda se puede realizar a través de metadatos (nombre de la empresa, nombre de dominio y correo electrónico). Debido a la presión persistente de Microsoft, incluso tenemos que eliminar nuestra página de consulta Este Día.

"En esta página de consulta, las empresas pueden ver si sus datos se publican de forma anónima en cualquier depósito abierto. Puede considerarlo como una versión B2B de havelbeenpwned. Los datos filtrados no nos pertenecen, por lo que no conservamos ningún dato.

"Estamos muy decepcionados con los comentarios y las acusaciones de MSRC después de toda la cooperación y el apoyo brindados por nosotros que impidieron absolutamente el desastre cibernético global".



## RECOMENDACIONES

- Validar si la información de su empresa no fue expuesta utilizando Bluebleed.
- Se recomienda mantener monitoreo constante sobre posibles boletines futuros emitidos por Microsoft referente a este tema y acatar recomendaciones.

## NOTICIA COMPLETA

<https://devel.group/blog/microsoft-expone-la-informacion-de-contacto-y-los-correos-electronicos-de-los-clientes/>

## ENLACE A BLUEBLEED

<https://socradar.io/labs/bluebleed>



## CONTACTOS DE SOPORTE



Correo electrónico: [cert@develsecurity.com](mailto:cert@develsecurity.com)

### Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: <https://www.devel.group/reporta-un-incidente>