

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

SECURITY OPERATIONS CENTER

**DESCUBIERTA VULNERABILIDAD CRÍTICA EN  
MICROSOFT OUTLOOK QUE PERMITE LA EJECUCIÓN  
REMOTA DE CÓDIGO**

13 / 06 / 2024

## CONTENIDO

INTRODUCCIÓN .....	3
RESUMEN .....	5
NOTICIA COMPLETA .....	6
CONTACTOS DE SOPORTE .....	7

## INTRODUCCIÓN

Recientemente, se ha descubierto una vulnerabilidad crítica en Microsoft Outlook, designada como CVE-2024-30103, que permite la ejecución remota de código sin necesidad de interacción del usuario. Este fallo de seguridad, debido a su naturaleza de "Zero-Click", representa una amenaza significativa, ya que los atacantes pueden comprometer un sistema simplemente enviando un correo electrónico especialmente diseñado y explotando la vulnerabilidad cuando el destinatario abre el mensaje. Dada la amplia utilización de Microsoft Outlook en entornos corporativos y personales, es crucial que los usuarios y administradores tomen medidas inmediatas para proteger sus sistemas contra esta seria amenaza.

## DESCUBIERTA VULNERABILIDAD CRÍTICA EN MICROSOFT OUTLOOK QUE PERMITE LA EJECUCIÓN REMOTA DE CÓDIGO

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

ID de alerta:	DSOC-CERT_2024_01_31_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	<b>CLEAR</b>
Fecha de publicación:	12/06/2024
Es día cero (0 day):	Sí

## RESUMEN


Se ha descubierto una vulnerabilidad crítica en Microsoft Outlook que permite la ejecución remota de código sin necesidad de interacción del usuario. Esta vulnerabilidad, designada como CVE-2024-30103, permite a los atacantes ejecutar código arbitrario simplemente enviando un correo electrónico especialmente diseñado. Cuando el destinatario abre el correo, se desencadena el exploit.

### Microsoft Outlook Remote Code Execution Vulnerability New

CVE-2024-30103  
Security Vulnerability

**Released: Jun 11, 2024**


**Assigning CNA:** Microsoft

[CVE-2024-30103](#) 

**Impact:** Remote Code Execution   **Max Severity:** Important

**Weakness:** CWE-184: Incomplete List of Disallowed Inputs

**CVSS Source:** Microsoft

**CVSS:3.1 8.8 / 7.7** 

## DETALLES DE LA VULNERABILIDAD

La vulnerabilidad CVE-2024-30103 es particularmente alarmante debido a su naturaleza de “Zero-Click”. A diferencia de los ataques de phishing tradicionales que requieren alguna acción por parte del usuario, esta falla puede ser explotada sin ninguna acción del usuario. Simplemente abrir el correo electrónico malicioso es suficiente para comprometer el sistema, convirtiéndose en una herramienta poderosa para los ciberdelincuentes y reduciendo significativamente las barreras para una explotación exitosa.

## ANÁLISIS TÉCNICO

La vulnerabilidad reside en la manera en que Microsoft Outlook procesa ciertos componentes de los correos electrónicos. Al abrir un correo electrónico especialmente diseñado, se desencadena un desbordamiento de búfer que permite al atacante ejecutar código arbitrario con los mismos privilegios que el usuario que ejecuta Outlook. Esto puede llevar a un compromiso total del sistema, robo de datos o la propagación de malware dentro de una red.

## IMPACTO Y MITIGACIÓN

Dado el uso generalizado de Microsoft Outlook en entornos corporativos y personales, el impacto potencial de CVE-2024-30103 es vasto. Las organizaciones están particularmente en riesgo, ya que una explotación exitosa podría resultar en brechas de datos significativas, pérdidas financieras y daños reputacionales.

Microsoft ha reconocido la vulnerabilidad y ha lanzado un parche de seguridad para abordar el problema. Se recomienda encarecidamente a los usuarios y administradores que apliquen las últimas actualizaciones para mitigar el riesgo. Además, soluciones robustas de filtrado y monitoreo de correo electrónico pueden ayudar a detectar y bloquear correos electrónicos maliciosos antes de que lleguen a los usuarios finales.

## RECOMENDACIONES DE EXPERTOS

Los expertos en ciberseguridad han enfatizado la naturaleza crítica de esta vulnerabilidad. “Las vulnerabilidades de Zero-Click son particularmente peligrosas porque no requieren interacción del usuario, lo que las hace altamente efectivas para los atacantes,” dijo un portavoz de Morphisec. “Las organizaciones deben priorizar la aplicación de parches y adoptar un enfoque de seguridad en capas para protegerse contra amenazas tan sofisticadas.”

## ESTADO ACTUAL

Hasta las últimas actualizaciones, no se conocen ataques en circulación que exploten la vulnerabilidad de Microsoft Outlook CVE-2024-30103. Sin embargo, dada la gravedad de la vulnerabilidad, es crucial que las organizaciones actúen rápidamente para proteger sus sistemas y datos.

## NOTICIA COMPLETA

<https://devel.group/blog/descubierta-vulnerabilidad-critica-en-microsoft-outlook-que-permite-la-ejecucion-remota-de-codigo/>

## 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>