| | |
|---|---|
| Alerta de seguridad informática | 9VSA20-00126-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 20 de Enero de 2020 |
| Última revisión | 20 de Enero de 2020 |

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Microsoft referente a una vulnerabilidad de corrupción de memoria presente en el motor de secuencias de comandos de Microsoft Internet Explorer el cual puede permitir que un atacante remoto no autenticado ejecute código arbitrario

## Vulnerabilidad

CVE-2020-0674

## Impacto

Microsoft Internet Explorer contiene un motor de secuencias de comandos que maneja la ejecución de lenguajes de secuencias de comandos como VBScript y JScript. El componente JScript del motor de secuencias de comandos contiene una vulnerabilidad de corrupción de memoria no especificada. Cualquier aplicación que admita incrustar Internet Explorer o su componente del motor de secuencias de comandos puede usarse como un vector de ataque para esta vulnerabilidad.

Un atacante que aprovechara la vulnerabilidad con éxito podría obtener los mismos derechos de usuario que el usuario actual. Si el usuario actual ha iniciado sesión con derechos de usuario administrativos, un atacante que haya explotado con éxito la vulnerabilidad podría tomar el control de un sistema afectado, permitiéndole instalar programas; ver, cambiar o eliminar datos; o crear nuevas cuentas con plenos derechos de usuario.

En un escenario de ataque basado en la web, un atacante podría alojar un sitio web especialmente diseñado para aprovechar la vulnerabilidad a través de Internet Explorer y luego convencer a un usuario para que vea el sitio web, por ejemplo, enviando un correo electrónico.

## Productos Afectados

Internet Explorer 9, 10, 11

## Mitigación

De forma predeterminada, Internet Explorer en Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 y Windows Server 2019 se ejecuta en un modo restringido que se conoce como Configuración de seguridad mejorada. La configuración de seguridad mejorada es un grupo de configuraciones preconfiguradas en Internet Explorer que puede reducir la probabilidad de que un usuario o administrador descargue y ejecute contenido web especialmente diseñado en un servidor. Este es un factor atenuante para los sitios web que no ha agregado a la zona de sitios de confianza de Internet Explorer.

## Solución Alternativa

Tenga en cuenta que la implementación de estos pasos puede resultar en una funcionalidad reducida para componentes o características que dependen de jscript.dll. Por ejemplo, dependiendo del entorno, esto podría incluir configuraciones de clientes que aprovechen los scripts de configuración automática del proxy (scripts PAC). Estas características y otras pueden verse afectadas.

Microsoft recomienda estos pasos de mitigación solo si hay indicios de que está bajo un riesgo elevado. Si implementa la solución alternativa, deberá revertir los pasos de mitigación antes de instalar cualquier actualización futura para continuar protegido.

De manera predeterminada, IE11, IE10 e IE9 usan Jscript9.dll que no se ve afectado por esta vulnerabilidad. Esta vulnerabilidad solo afecta a ciertos sitios web que utilizan jscript como motor de secuencias de comandos.

## Restringir el acceso a JScript.dll

En sistemas de 32-bit, ejecutar los siguientes comandos en una consola de administración (command prompt):

```
takeown /f %windir%\system32\jscript.dll
cacls %windir%\system32\jscript.dll /E /P everyone:N
```

En sistemas de 64-bit, ejecutar los siguientes comandos en una consola de administración (command prompt):

```
takeown /f %windir%\syswow64\jscript.dll
cacls %windir%\syswow64\jscript.dll /E /P everyone:N
takeown /f %windir%\system32\jscript.dll
cacls %windir%\system32\jscript.dll /E /P everyone:N
```

Para revertir los cambios

En sistemas de 32-bit, ejecutar los siguientes comandos en una consola de administración (command prompt):

```
cacls %windir%\system32\jscript.dll /E /R everyone
```

En sistemas de 64-bit, ejecutar los siguientes comandos en una consola de administración (command prompt):

```
cacls %windir%\system32\jscript.dll /E /R everyone
cacls %windir%\syswow64\jscript.dll /E /R everyone
```

Enlace

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200001
https://kb.cert.org/vuls/id/338824/

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.01.20 21:06:39 -03'00'