# USTIC-AV 15/22. Los parches de seguridad de Microsoft Windows de octubre corrigen 13 vulnerabilidades críticas, incluidas 2 de día cero (13/10 /2022)

La **Unidad de Seguridad TIC** de la Subdirección de Tecnologías de la Información y Comunicaciones **avisa** de que han sido **liberados los parches de seguridad mensuales de Microsoft Windows de octubre que corrigen,** entre otras, **13 vulnerabilidades críticas, incluidas 2 de día cero conocidas, una de las cuales estaba siendo explotada activamente**.

Asimismo, en el apartado correspondiente en este comunicado, se informa del **calendario del despliegue desde Altiris** de estos parches para puestos de usuarios.

**Respecto a los servidores afectados, se ruega a sus responsables la máxima diligencia en su resolución**, debido al riesgo potencial que presentan estas vulnerabilidades.

## Detalle

Microsoft ha lanzado su nueva ronda de actualizaciones para Windows en su boletín mensual de octubre, corrigiendo 84 vulnerabilidades, 13 de ellas clasificadas como críticas (dos son de Día Cero o *0-day*), ya que, alternativa o conjuntamente, permiten la elevación de privilegios del sistema, la suplantación de identidad o la ejecución remota de código

El número de vulnerabilidades en cada categoría se enumeran de la siguiente forma:

- 39 de elevación de privilegios.
- 2 de omisión de características de seguridad.
- 20 de ejecución remota de código.
- 11 de divulgación de información.
- 8 de denegación de servicio.
- 4 de suplantación de identidad.

Los principales fallos que resuelven las actualizaciones son los siguientes:

  - CVE-2022-41033: Vulnerabilidad de día cero, explotada activamente. Se debe a un fallo de elevación de privilegios del Servicio del sistema de eventos COM+ de Windows (puntuación CVSS: 7,8).
  - CVE-2022-41043 : Vulnerabilidad *0-day* de divulgación de información de Microsoft Office que los atacantes podrían aprovechar para obtener acceso a los tokens del usuario y, desde allí, entrar a otros lugares del sistema.

Debido al riesgo potencial que presentan estas vulnerabilidades, llamamos vuestra atención sobre la urgencia de aplicar las recomendaciones indicadas y la adopción de medidas tan pronto como sea posible.

Desafortunadamente, Microsoft no ha publicado las actualizaciones de seguridad para las dos vulnerabilidades de día cero explotadas activamente y rastreadas como CVE-2022-41040 y CVE-2022-41082, también denominadas como "*ProxyNotShe*l", que ya fueron comunicadas a principios de este mes de octubre aquí.

## Sistemas Afectados

- Windows 7.
- Windows 8.1
- Windows 10
- Windows 11.
- Windows Server 2008 y 2008 R2.
- Windows Server 2012 y 2012 R2.
- Windows Server 2016.
- Windows Server 2019.
- Windows Server 2022.

## Recomendaciones Actualizadas (13/10/2022)

---

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones recomienda encarecidamente aplicar los siguientes pasos, con el fin de evitar la exposición a ataques externos y la toma de control de los sistemas informáticos:

# Mitigación

**1º. Solución a las vulnerabilidades:**

Será necesario **implementar los parches** liberados lo antes posible.

## Despliegue de Parches desde Altiris para Equipos de Usuarios. Calendario.

---

El despliegue de los parches de seguridad de los equipos de usuario se realizará desde Altiris de manera escalonada, por anillos, atendiendo al siguiente calendario:

- Anillo 1: 18 de octubre
- Anillo 2: 25 de octubre
- Anillo 3: 2 de noviembre

Desde el punto de vista del impacto en los usuarios, esta actualización, una vez instalada, informará al usuario que debe reiniciar el equipo.

## Referencias

- October 2022 Security Updates
- Security Update Guide

Para cualquier duda o consulta al respecto, puede ponerse en contacto con nuestro equipo en ustic.stic.sspa@juntadeandalucia.es.

Gracias por vuestra atención.

**Unidad de Seguridad TIC**

**Subdirección de Tecnologías de la Información y Comunicaciones**

**Servicio Andaluz de Salud**