Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

PATCH TUESDAY JUNIO 2025: SE CORRIGEN VULNERABILIDADES BAJO ATAQUE ACTIVO

12 / 06 / 2025

CONTENIDO

INTRODUCCIÓN

Este mes, Microsoft ha lanzado su importante boletín de seguridad conocido como "Patch Tuesday", abordando un total de 66 vulnerabilidades en sus productos. Estas actualizaciones son cruciales, ya que incluyen correcciones para 25 vulnerabilidades de ejecución remota de código, 17 de divulgación de información, 13 de elevación de privilegios, 6 de denegación de servicio, 3 de omisión de funciones de seguridad y 2 de suplantación de identidad.

PATCH TUESDAY JUNIO 2025: SE CORRIGEN VULNERABILIDADES BAJO ATAQUE ACTIVO

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

ID de alerta:	DSOC-CERT_2025_06_12_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	11/06/2025
Es día cero (0 day):	Sí

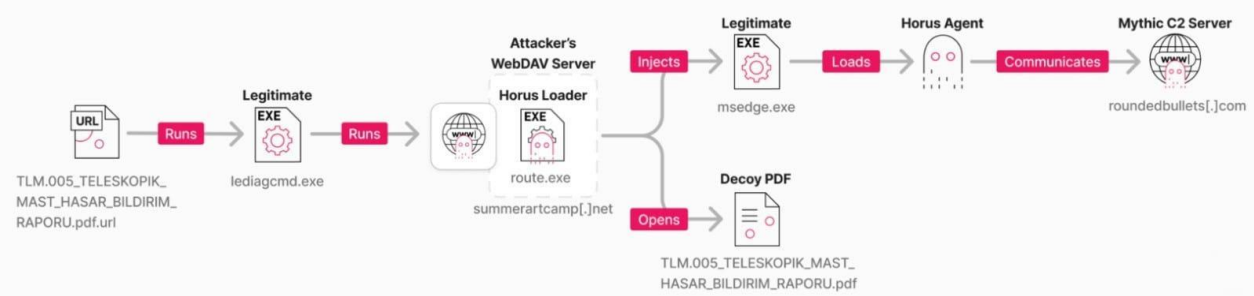
RESUMEN

La empresa Microsoft lanzó una importante cantidad de actualizaciones para vulnerabilidades que estaban siendo explotadas, a este boletín se le conoce como: Patch Tuesday. Estas actualizaciones cubren un total de 66 vulnerabilidades y se dividen de la siguiente forma:

- 25 vulnerabilidades de ejecución remota de código
- 17 vulnerabilidades de divulgación de información
- 13 vulnerabilidades de elevación de privilegios
- 6 vulnerabilidades de denegación de servicio
- 3 vulnerabilidades de omisión de funciones de seguridad
- 2 vulnerabilidades de suplantación de identidad
-

Dentro de estas vulnerabilidades se incluyen 2 de tipo zero-day que se encontraban siendo explotadas por los atacantes, una de ellas fue divulgada públicamente, Se clasifican de esta forma por Microsoft cuando no se tiene una solución inmediata. Las vulnerabilidades de zero-day son las siguientes:

CVE-2025-33053: Esta es una vulnerabilidad que permite al atacante remoto correr código arbitrario hacia el sistema afectado en este caso Microsoft Windows Web Distributed Authoring and Versioning (WEBDAV) se requiere que el usuario haga clic en una url de WEBDAV específicamente modificada para que la falla sea explotada.

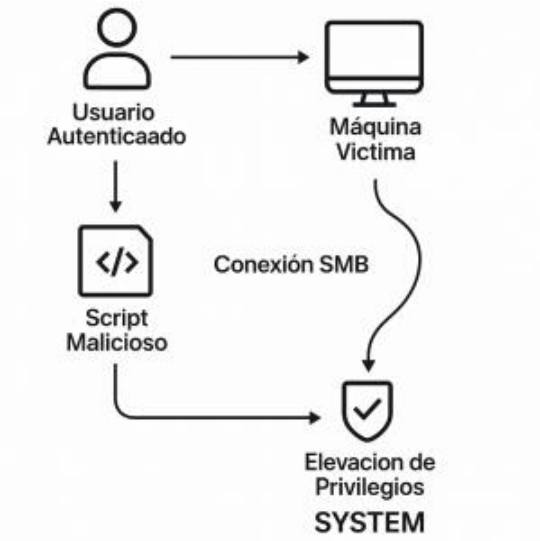


Esta fue explotada por un grupo conocido como: Stealth Falcon. Son un grupo de atacantes que se centran en Medio Oriente y África, sus objetivos tienen a ser personas importantes en los ámbitos gubernamentales, algunos ejemplos de países son: Turquía, Qatar y Yemen.

Son conocidos por utilizar el método de ataque spear phishing. Esto es enviar phishing dirigido a un individuo o grupo selecto de personas utilizando información personal para que crean que es legítimo, esto va muy de la mano con hacer ingeniería social para la víctima.

CVE-2025-33073: Esta es una vulnerabilidad de elevación de privilegios dirigida hacia el sistema SMB de Windows. ¿Qué es SMB? A simples rasgos es un protocolo de red que permite enviar archivos y otros recursos entre computadoras. Lo utilizan las empresas para los archivos compartidos. La falla se debe a un control inadecuado de los permisos en ciertas circunstancias.

El atacante en cuestión crea un script malicioso especialmente diseñado para obligar a la maquina a conectarse nuevamente al sistema de ataque mediante el protocolo SMB y así autenticarse, esto resulta en una elevación de privilegios. Microsoft no relevo información de cómo se encontró la falla.



VULNERABILIDADES CRITICAS DEL PACTH TUESDAY DE MICROSOFT

Estas son las vulnerabilidades con criticidad más alta de las 66 actualizadas.

Servicio	CVE ID	Titulo	Criticidad
Microsoft Office	CVE-2025-47164	Vulnerabilidad de ejecución remota de código de Microsoft Office	**Crítico**
Microsoft Office	CVE-2025-47167	Vulnerabilidad de ejecución remota de código de Microsoft Office	**Crítico**
Microsoft Office	CVE-2025-47162	Vulnerabilidad de ejecución remota de código de Microsoft Office	**Crítico**
Microsoft Office	CVE-2025-47953	Vulnerabilidad de ejecución remota de código de Microsoft Office	**Crítico**

Microsoft Office SharePoint	CVE-2025-47172	Vulnerabilidad de ejecución remota de código de Microsoft SharePoint Server	**Crítico**
Servicios criptográficos de Windows	CVE-2025-29828	Vulnerabilidad de ejecución remota de código de Windows Schannel	**Crítico**
Servicio de proxy KDC de Windows (KPSSVC)	CVE-2025-33071	Vulnerabilidad de ejecución remota de código del servicio de proxy KDC de Windows (KPSSVC)	**Crítico**
Windows Netlogon	CVE-2025-33070	Vulnerabilidad de elevación de privilegios de Windows Netlogon	**Crítico**
Servicios de Escritorio remoto de Windows	CVE-2025-32710	Vulnerabilidad de ejecución remota de código de Servicios de Escritorio remoto de Windows	**Crítico**

RECOMENDACIONES

- **Aplicar las actualizaciones de inmediato**: Instale los parches de seguridad tan pronto como estén disponibles para proteger sus sistemas de vulnerabilidades críticas, especialmente las de ejecución remota de código y elevación de privilegios.
- **Revisar configuraciones de seguridad**: Verifique las configuraciones de servicios clave como RDP, LDAP y Windows Defender Credential Guard para evitar que nuevos vectores de ataque sean explotados.
- **Monitorear sistemas y redes**: Utilice herramientas de detección y respuesta ante amenazas (EDR/XDR) para identificar actividad sospechosa y prevenir la explotación de vulnerabilidades no corregidas.
- **Fortalecer políticas de acceso**: Implemente autenticación multifactor (MFA) y restrinja el acceso a sistemas críticos solo a usuarios autorizados.

- **Actualizar todos los componentes de software**: Aplique las actualizaciones no solo al sistema operativo, sino también a productos como Microsoft Edge y Office.
- **Educación en ciberseguridad**: Capacite a los usuarios sobre las mejores prácticas de seguridad, especialmente sobre cómo evitar enlaces y archivos sospechosos.

NOTICIA COMPLETA

https://devel.group/blog/patch-tuesday-junio-2025-se-corrigen-vulnerabilidades-bajo-ataque-activo/

CONTACTOS DE SOPORTE

Correo electrónico: cti@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://devel.group