BOLETÍN DE ALERTA

Boletín Nro.: 2020-01
Fecha de publicación: 16/01/2020
Tema: Actualizaciones de seguridad críticas y no críticas en Windows

Las vulnerabilidades declaradas como críticas, son: **CVE-2020-0609 - CVE-2020-0610 - CVE-2020-0601**

Además, existen vulnerabilidades que han sido declaradas como importantes:

CVE-2020-0607- CVE-2020-0608 - CVE-2020-0615 - CVE-2020-0622 - CVE-2020-0637 - CVE-2020-0639 - CVE-2020-0643 - CVE-2020-0647 - CVE-2020-0650 - CVE-2020-0651 - CVE-2020-0652 - CVE-2020-0653 - CVE-2020-0654

Sistemas afectados por las vulnerabilidades críticas:

Las vulnerabilidades críticas, CVE-2020-0609 y CVE-2020-0610 afectan a las siguientes versiones de Windows:

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

Para el CVE-2020-0601 se ven afectadas las siguientes versiones:

- Microsoft Windows 10, en varias versiones o ediciones. Ver listado aquí
- Microsoft Windows Server 2016 y Windows Server 2016 (instalación de Server Core).
- Microsoft Windows Server 2019 y Windows Server 2019 (instalación de Server Core).

Sistemas afectados por las vulnerabilidades no críticas:

- Microsoft Windows;
- Internet Explorer;
- Microsoft Office, Microsoft Office Services y Web Apps;
- ASP.NET Core;
- .NET Core;
- .NET Framework;
- OneDrive para Android;
- Microsoft Dynamics;

Descripción

Windows Remote Desktop Gateway o también conocido como RD Gateway es el componente que proporciona acceso a los servicios de escritorio remoto, con el fin de que usuarios externos puedan acceder a los recursos internos de la organización. Para asegurar las comunicaciones de escritorio remoto, los clientes que inicializan la comunicación deben establecer un canal seguro con la puerta de enlace de RD a través de un túnel SSL. Luego, RD Gateway necesita asegurarse de que el cliente sea un usuario de escritorio remoto válido, esto inicializa la conexión RDP con los backends que entregan los recursos internos. En otras palabras, el RD Gateway actúa como un proxy RD entre el cliente y los

recursos internos.

La falla se da porque, la **Puerta de Enlace de RD** no realiza una validación correcta de la solicitud de los servicios RDP destino, permitiendo a atacante no autenticado enviar solicitudes especialmente diseñadas y así activar la ejecución arbitraria código en el sistema de destino, cabe destacar que esta ejecución de código se produce a nivel del servidor, el cual se da previa a la autenticación y sin interacción del usuario.

Un atacante que logre explotar exitosamente esta vulnerabilidad, podría instalar programas maliciosos; ver, cambiar o eliminar datos; crear cuentas de usuarios y tomar el control total del recurso afectado, por otro lado los intentos fallidos de esta explotación podrían causar una denegación de servicio.

Por otro lado, la NSA ha descubierto una vulnerabilidad en la funcionalidad de Windows CryptoAPI, la cual se encarga de la criptografía, en otras palabras es una interfaz que permite a los desarrolladores firmar su software para garantizar que no ha sido modificado y que proviene de fuentes seguras.

En este caso la falla se da en la forma que el componente **crypt32.dll** valida los certificados de criptografía de curva elíptica (ECC), un atacante podría aprovechar esta vulnerabilidad para firmar un archivo ejecutable malicioso usando un certificado de firma falso, con esto se puede hacer creer a la víctima que el archivo proviene de una fuente confiable. Además un atacante podría realizar ataques MITM y descifrar información confidencial sobre las conexiones de los usuarios con el software afectado.

Microsoft ha declarado que hasta ahora no han visto una explotación activa de estas vulnerabilidades, ni la existencia de un exploit público para las mismas. Sin embargo, las vulnerabilidades están etiquetadas como '**Explotación más probable**'.

En el mismo paquete de actualizaciones, Microsoft ha corregido otras vulnerabilidades importantes que afectan a distintos productos de Microsoft. Ver listado aquí.

Impacto:

Un atacante podría:

- instalar programas maliciosos, ver, cambiar o eliminar datos, crear cuentas de usuarios y tomar el control total del recurso afectado.
- firmar un ejecutable malicioso, realizar ataques MITM y descifrar información confidencial sobre las conexiones de los usuarios con el software afectado.
- divulgar de información,
- escalar de privilegios,
- causar denegación de servicio,
- ejecutar códigos remotos.
- suplantar de identidades, etc.

Solución y Prevención:

Microsoft ha publicado actualizaciones de software para abordar las vulnerabilidades críticas CVE-2020-0601, CVE-2020-0609 y CVE-2020-0610. Se recomienda su aplicación en los distintos sistemas operativos. Las mismas se pueden encontrar en los siguientes enlaces:

- https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-0609
- https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-0610
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601

Además, como medida preventiva se recomienda:

- Ejecutar todo el software como un usuario sin privilegios con derechos de acceso mínimos.
- Implementar sistemas de detección de intrusos en la red y monitorear el tráfico de la red en busca de actividad maliciosa.
- No aceptar ni ejecutar archivos de fuentes desconocidas o que no sean de confianza.
- Enrutan el tráfico a través de dispositivos proxy, que realizan la inspección TLS.
- Utilizar herramientas de análisis de captura de paquetes, como Wireshark, para analizar y extraer los certificados, y así determinar su validez.

Además para las vulnerabilidades críticas CVE-2020-0601 y CVE-2020-0609 se recomienda no publicar el protocolo RDP hacia internet, si es necesario acceder por RDP es recomendable hacerlo mediante una conexión VPN.

Para las vulnerabilidades importantes CVE-2020-0607, CVE-2020-0608, CVE-2020-0615, CVE-2020-0622, CVE-2020-0637, CVE-2020-0639, CVE-2020-0643, CVE-2020-0647, CVE-2020-0650, CVE-2020-0651, CVE-2020-0652, CVE-2020-0653, CVE-2020-0654, se recomienda aplicar las actualizaciones de seguridad tan pronto como sea posible.

Información adicional:

- https://nvd.nist.gov/vuln/detail/CVE-2020-0609
- https://nvd.nist.gov/vuln/detail/CVE-2020-0610
- https://nvd.nist.gov/vuln/detail/CVE-2020-0601
- https://media.defense.gov/2020/Jan/14/2002234275/-1/-1/0/CSA-WINDOWS-10-CRYPT-LIB-20190114.PDF
- https://www.symantec.com/security-center/vulnerabilities/writeup/111368