Una nueva técnica de ataque podría permitir eludir la Aplicación de Firmas de Controladores (DSE) de Microsoft en sistemas Windows completamente actualizados, lo que facilitaría ataques de degradación del sistema operativo.

> *«Este método permite cargar controladores de kernel sin firmar, proporcionando a los atacantes la posibilidad de implementar rootkits personalizados que neutralicen controles de seguridad, oculten procesos y actividad en la red, mantengan el sigilo y más»*, indicó el investigador de SafeBreach, Alon Leviev.

Los descubrimientos recientes se basan en un análisis previo que identificó dos fallos de escalada de privilegios en el proceso de actualización de Windows (CVE-2024-21302 y CVE-2024-38202) que podrían utilizarse para revertir una instalación actualizada de Windows a una versión anterior con vulnerabilidades de seguridad sin resolver.

El exploit toma forma en una herramienta llamada Windows Downdate, que, según Leviev, podría utilizarse para manipular el proceso de actualización de Windows, generando degradaciones irreversibles y sin detección en componentes críticos del sistema operativo.

Esto plantea riesgos graves, ya que ofrece a los atacantes una alternativa mejorada a los ataques de «Bring Your Own Vulnerable Driver» (BYOVD), permitiéndoles degradar módulos principales de Windows, incluido el núcleo del sistema.

Microsoft abordó las vulnerabilidades CVE-2024-21302 y CVE-2024-38202 el 13 de agosto y el 8 de octubre de 2024, respectivamente, como parte de sus actualizaciones de Patch Tuesday.

El último método ideado por Leviev utiliza la herramienta Windows Downdate para degradar el parche de bypass de DSE *«ItsNotASecurityBoundary»* en un sistema Windows 11 totalmente actualizado.

ItsNotASecurityBoundary fue documentado por primera vez por el investigador de Elastic

Security Labs, Gabriel Landau, en julio de 2024 junto con PPLFault, describiéndolos como una nueva clase de fallos llamada False File Immutability. Microsoft corrigió este fallo en mayo de este año.

En resumen, la técnica explota una condición de carrera para sustituir un archivo de catálogo de seguridad verificado por una versión maliciosa que contiene una firma de autenticode para un controlador de kernel sin firmar, tras lo cual el atacante solicita al kernel que cargue dicho controlador.

El sistema de integridad de código de Microsoft, que verifica un archivo a través de la biblioteca de modo kernel ci.dll, analiza el catálogo de seguridad malicioso para validar la firma del controlador y cargarlo, permitiendo al atacante ejecutar código arbitrario en el kernel.

El bypass de DSE se logra usando la herramienta de degradación para reemplazar la biblioteca «ci.dll» con una versión anterior (10.0.22621.1376) y así revertir el parche de Microsoft.

Dicho esto, existe una barrera de seguridad que puede impedir que este bypass funcione. Si la Seguridad Basada en Virtualización (VBS) está habilitada en el sistema de destino, el escaneo del catálogo es realizado por la DLL de Integridad de Código del Kernel Seguro (skci.dll), en lugar de ci.dll.

Sin embargo, la configuración predeterminada es VBS sin bloqueo de la Interfaz de Firmware Extensible Unificada (UEFI), lo que permite a un atacante desactivarla modificando las claves de registro EnableVirtualizationBasedSecurity y RequirePlatformSecurityFeatures.

Incluso si el bloqueo UEFI está activado, el atacante podría deshabilitar VBS reemplazando uno de los archivos principales por una versión no válida. En última instancia, los pasos para llevar a cabo el ataque son los siguientes:

1. Desactivar VBS en el Registro de Windows o invalidar SecureKernel.exe.
2. Degradar ci.dll a la versión sin parche.
3. Reiniciar el sistema.
4. Exploitar el bypass DSE de ItsNotASecurityBoundary para ejecutar código a nivel de kernel.

El único caso en el que falla es cuando VBS está habilitado con bloqueo UEFI y una opción de «Obligatorio» (Mandatory), que provoca un fallo de arranque si los archivos de VBS están dañados. El modo Obligatorio se activa manualmente mediante un cambio en el registro.

> *«La configuración Obligatoria evita que el cargador del sistema operativo continúe iniciándose si el hipervisor, el kernel seguro o uno de sus módulos dependientes no se carga. Es importante ser cuidadoso al habilitar este modo, ya que, si algún módulo de virtualización falla, el sistema no podrá arrancar»,* explica Microsoft en su documentación.

Por lo tanto, para mitigar completamente el ataque, es esencial que VBS esté activado con bloqueo UEFI y la opción Obligatoria habilitada. En cualquier otra configuración, un atacante podría desactivar esta función de seguridad, degradar la DLL y realizar el bypass de DSE.

> *«La conclusión principal [...] es que las soluciones de seguridad deberían intentar detectar y prevenir procedimientos de degradación incluso para componentes que no cruzan límites de seguridad definidos»*, comentó Leviev.