BOLETÍN DE ALERTA

Boletín Nro.: 2021-18
Fecha de publicación: 18/08/2021
Tema: Múltiples debilidades críticas de Sistemas Windows en configuración por defecto

Sistemas afectados:

Todos los siguientes sistemas operativos están afectados por al menos una de las problemáticas descritas en el siguiente boletín:

- Windows 10
- Windows 8 / 8.1
- Windows 7
- Windows Server 2004
- Windows Server 2008
- Windows Server 2012
- Windows Server 2016
- Windows Server 2019
- Windows RT 8.1

Descripción:

En las últimas semanas se han descubierto diversas vulnerabilidades críticas y nuevas técnicas de ataque a diversos componentes de sistemas Windows. La mayoría de estas vulnerabilidades y ataques se han documentado en entornos en su configuración por defecto y se deben a debilidades o fallas de diseño.

Las vulnerabilidades y/o técnicas de ataque son las siguientes:

Vulnerabilidad / Ataque	CVE asignado	Explotación	Táctica / Impacto	
Ataque de retransmisión PetitPotam NTLM	CVE-2021-36942	Remotamente (red interna)	Movimiento Lateral	Windows Server 2008 Windows Server 2008 R2 Windows Server 2016 Windows Server 2019 Windows Server 2022

Vulnerabilidad de escalada de privilegios en el protocolo RPC de Windows (RemotePotato0)	N/A (funcionalidad)	Local	Escalación de privilegio	IIS 6.0 a IIS 10.0 Windows 10
Abuso de los servicios de certificados de Active Directory (ADCS - ESC8)	N/A (funcionalidad)	Remotamente (red interna)	Movimiento Lateral y escalación de privilegios	Windows y Windows Server, todas las versiones desde 2008
Forzar autenticación privilegiada NTLM (SpoolSample)	N/A (funcionalidad)	Remotamente (red interna) y local	Movimiento Lateral y escalación de privilegios	Windows y Windows Server, todas las versiones
Vulnerabilidad de elevación de privilegios de Windows (SeriousSAM)*	CVE-2021-36934	Local	Escalación de privilegios	Windows 10
Vulnerabilidad de RCE y LPE en el servicio Print Spooler de Microsoft Windows (PrintNightmare)**	RCE: CVE-2021-1675, CVE-2021-34527, CVE-2021-36936, CVE-2021-36947 CVE-2021-36958 LPE: CVE-2021-34481 CVE-2021-34483	Remotamente (red interna)	Ejecución remota de código y Escalación de privilegios	Windows y Windows Server, todas las versiones

* Abordado en el boletín BOL-CERT-PY-2021-17
** Abordado en el boletín BOL-CERT-PY-2021-15

Recientemente en el último parche de seguridad de Microsoft se abordaron e introdujeron mitigaciones para algunas de las vulnerabilidades, pero no todas. El último parche incluye correcciones y/o mitigaciones para 44 vulnerabilidades

Sin embargo, como muchas de las técnicas de ataques descritas se basan en un conjunto de condiciones, estos parches abordan solo parcialmente las vulnerabilidades y en la mayoría de los casos es necesario que los propios administradores apliquen medidas de mitigación adicionales.

A continuación, puede encontrar el detalle de cada una de las problemáticas mencionadas:

1. **Ataque de retransmisión PetitPotam NTLM**

   Se trata de una nueva variante de la técnica de ataque de retransmisión NTLM (NTLM-relay) mediante la cual se le fuerza a un sistema Windows a autenticarse en otras máquinas a través de la función MS-EFSRPC EfsRpcOpenFileRaw.

   El atacante envía solicitudes SMB a la interfaz MS-EFSRPC de un sistema remoto y obliga a la computadora víctima a iniciar un procedimiento de autenticación y

compartir su hash de autenticación NTLM. Si el ataque se realiza contra una controladora de dominio (DC), puede llegar a comprometer todo el dominio.

Cabe destacar que el atacante no necesita credenciales ni interacción del usuario para que el ataque tenga éxito.

Un equipo es potencialmente vulnerable si la autenticación NTLM está habilitada en su dominio y se están utilizando los Servicios de certificados de Active Directory (AD CS) con cualquiera de los siguientes servicios:

- Inscripción web de la autoridad de certificación.
- Servicio web de inscripción de certificados.

Afecta a todas las versiones de Windows Server, desde 2008 hasta 2022. La vulnerabilidad en la que se basa parcialmente esta técnica fue identificada como CVE-2021-36942.

2. **Vulnerabilidad de escalada de privilegios en el protocolo RPC de Windows (RemotePotato0)**

RemotePotato0 es una nueva variante de la técnica de retransmisión NTLM, que se basa en el abuso del servicio de activación RPC/DCOM y dispara una autenticación NTLM de cualquier usuario actualmente logueada en la máquina víctima, contactando a un servidor RPC controlado por el atacante.

El mensaje NTLM tipo 1 privilegiado es retransmitido, el paquete de autenticación RPC desempaquetado y encapsulado en un paquete HTTP que es retransmitido a algún servidor privilegiado (LDAP, SMB, HTTP u otro). En el caso de la Prueba de Concepto construida por los investigadores que publicaron originalmente la técnica, se retransmite la autenticación NTLM al servidor LDAP que se ejecuta en la controladora de dominio para añadir un nuevo administrador de dominio o escalar de privilegios.

El ataque es posible cuando se dan las siguientes condiciones:

- Un usuario con privilegios de Administrador de Dominio está en el equipo, ya sea físicamente o mediante Escritorio Remoto (RDP).
- El atacante ha ganado acceso inicial al equipo
- No se ha configurado LDAP y SMB Signing

Al igual que PetitPotam, el atacante no necesita credenciales ni interacción del usuario para que el ataque tenga éxito.

3. Abuso de los servicios de certificados de Active Directory (ADCS - ESC8)

El servicio de certificado de Active Directory (ADCS) soporta varios métodos de enrolamiento basado en HTTP mediante roles de servidor adicionales que un administrador puede instalar. Recientemente se descubrió que todas estas interfaces de enrolamiento de certificados web, en su configuración por defecto, son vulnerables a ataques de retransmisión NTLM.

Un atacante puede retransmitir la autenticación de usuario/máquina a la interfaz web del servidor AD CS y solicitar un certificado en nombre de la cuenta retransmitida. Una vez que el atacante obtiene el certificado, puede solicitar un token de autenticación TGT (*Ticket Granting Ticket - Kerberos*) e impersonificar a ese usuario/máquina en la red.

El ataque, al igual que cualquier ataque de retransmisión NTLM clásico, requiere una cuenta víctima que se autentique en la máquina controlada por el atacante; éste puede forzar la autenticación de múltiples maneras, como por ejemplo mediante el método MS-RPRN *RpcRemoteFindFirstPrinterChangeNotification(Ex)*, mediante la técnica/herramienta “SpoolerSample” o en combinación con la técnica PetitPotam.

La técnica puede ser utilizada para obtener el certificado de cualquier usuario o servidor Windows, incluido el controlador de dominio. En este último caso, el atacante obtiene el control total de todo el dominio.

ADCS no se encuentra instalado por defecto en entornos de Active Directory, sin embargo, es un servicio ampliamente utilizado en organizaciones

.

4. Forzar autenticación privilegiada NTLM (SpoolSample)

Microsoft Print System Remote Protocol (MS-RPRN) permite a un usuario de dominio forzar a cualquier otra máquina en la que se ejecuta el servicio Spooler a conectarse a una segunda máquina con delegación irrestricta. La API RpcRemoteFindFirstPrinterChangeNotificationEx permite a clientes de impresora suscribirse a notificaciones de cambios en el servidor de impresión. Por defecto, el servicio Spool está habilidado en controladores de dominio.

Una llamada a esta API provocará que el servidor de impresión en la controladora a autenticarse a la máquina y proveerle el ticket de autenticación (TGT Kerberos) y almacenarse en el Local Security Authority Subsystem Service (LSASS).

SpoolSample abusa esta funcionalidad para forzar a un objetivo A a autenticarse en un destino elegido por los atacantes (objetivo B) a través de la interfaz MS-RPRN RPC. Este destino suele ser otro host en el que se ejecuta alguna herramienta de retransmisión NTLM (ej.: ntlmrelayx, inveigh u otra), que a su vez retransmite el objetivo A al objetivo final, el objetivo C. Los permisos del objetivo A se utilizan para ejecutar comandos o acciones arbitrarias en el destino C. El destino C podría ser el servicio LDAP de una Controladora de Dominio, permitiendo al atacante controlar el dominio completo.

Esta funcionalidad también puede ser abusada para escalar de privilegios localmente.

5. SeriousSAM

Tal como fue descrito en el boletín CERT-PY 2021-17, esta vulnerabilidad permite que un usuario no privilegiado pueda leer el contenido del Security Account Manager (SAM), donde se encuentran los hashes de usuarios locales, de dominio y/o otros usuarios cuyas credenciales se encuentran almacenadas en el equipo (por ej, los usuarios de TI que se han logueado en el pasado, para tareas de soporte). Esto permitiría a un atacante llevar a cabo un ataque del tipo Pass-the-Hash, para movimiento lateral entre sistemas.
El parche de seguridad publicado requiere acciones adicionales por parte de los administradores.

6. PrintNightmare

En el boletín CERT-PY 2021-16 se alertó acerca de vulnerabilidades críticas que afectan al servicio Print Spooler, sin embargo, en los días posteriores se siguió descubriendo otras vulnerabilidades que también lo afectaban. A ese conjunto de vulnerabilidades se le denominó PrintNightmare. Si bien, se trata de 7 vulnerabilidades técnicamente independientes y diferentes entre sí, todas ellas derivan en escalación de privilegios local o en ejecución remota de código.
Ejecución remota de código:

- CVE-2021-1675
- CVE-2021-34527
- CVE-2021-36936
- CVE-2021-36947

- CVE-2021-36958

Escalación de privilegios local:

- CVE-2021-34481
- CVE-2021-34483

Existe un parche completo para 5 de ellas: CVE-2021-1675, CVE-2021-36936, CVE-2021-36947, CVE-2021-34481, CVE-2021-34483
Para CVE-2021-34527 existe un parche parcial, pero que requiere una verificación y/o cambio de configuración adicional para funcionar.
Para CVE-2021-36958, publicado hace pocos días, no existe todavía parche. Ver la sección “Mitigación” para mayor información.

Mitigación:

En el parche de seguridad del martes 10 de agosto, Microsoft incluyó algunas actualizaciones que mitigan parcialmente alguna de las vulnerabilidades o debilidades que posibilitan las técnicas de ataques, entre ellas específicamente las siguientes:

- CVE-2021-36942 (PetitPotam) - el parche bloquea la interface LSARPC interface
- CVE-2021-36936, CVE-2021-36947 y CVE-2021-34483 (PrintNightMare)
- CVE-2021-34527 (PrintNightmare) - requiere acciones adicionales, ver detalles.

CVE-2021-1675 y CVE-2021-34481 ya habían sido abordadas en el parche de julio.
CVE-2021-36934 (SeriousSAM) ya había sido abordada en el parche de julio pero requiere acciones adicionales, ver detalles.
Se recomienda a todos los administradores actualizar todos los sistemas Windows (estaciones 8/10/11 y Server).

Como la mayoría de las problemáticas descritas en este boletín no se basan en errores de código sino debilidades de diseño y/ abuso de funcionalidades legítimas, este parche no evita, por sí solo, todas las técnicas de ataque descritas, por lo que se insta a los administradores implementar medidas de mitigación acorde a su arquitectura e infraestructura.

Si bien, las causas y condiciones que facilitan las técnicas de ataque descritas son diversas, y, en general, es posible implementar algunas medidas de mitigación transversales generales, entre ellas:

- Mitigar y reforzar al máximo la protección y defensas ante ataques de retransmisión NTLM (NTLM Relay attack), configurando y forzando las opciones de seguridad en servicios sensibles tales como Firma LDAP (LDAP Signing), Protección de enlace de canal (LDAP Channel binding) en Controladores de dominio y hardening en los servicios basados en IIS
- Prevenir que los servicios se autentiquen a estaciones de trabajo arbitrarias, filtrando o denegando el tráfico iniciado de servidores a estaciones de trabajo. Una lista blanca de conexiones requeridas puede ser utilizada en aquellos casos en que determinados servicios requieran necesariamente la conexión a ciertas estaciones de trabajo.
- Desactivar servicios poco seguros, cuyas funcionalidades pueden ser abusadas, siempre que sea posible (por ej: Spooler Service, WebClient)
- Configurar/Habilitar Extended Protection for Authentication (EPA) para todos los servicios que lo soportan
- Eliminar el uso del protocolo NTLM por completo, migrando a Kerberos.

A continuación, se describen las mitigaciones específicas adicionales para cada una de las problemáticas descritas:

1. PetitPotam:

   Activar Extended Protection for Authentication (EPA) con SSL y deshabilitar HTTP en los servidores AD CS.
   Adicionalmente, se recomienda deshabilitar autenticación NTLM en el controlador de dominio. Esto se puede lograr siguiendo la documentación en Seguridad de red: Restringir NTLM: autenticación NTLM en este dominio.
   En el caso de que no sea posible por razones de compatibilidad, se recomienda alguna de las siguientes acciones:

   - Desactive NTLM en cualquier servidor AD CS de su dominio mediante la política de grupo Seguridad de red: Restringir NTLM: tráfico NTLM entrante.
   - Deshabilite NTLM para Internet Information Services (IIS) en los servidores AD CS en el dominio que ejecuta los servicios de "Inscripción web de

autoridad de certificación" o "Servicio web de inscripción de certificados". (*Menos seguro*)

Las instrucciones detalladas se pueden encontrar en la guía KB5005413 de Microsoft: https://support.microsoft.com/en-us/topic/kb5005413

2. RemotePotat0:

- Para HTTP(s), se debe eliminar todos los enlaces HTTP no protegidos por TLS (preferentemente utilice SSL en todas partes, especialmente donde se usa NTLM) y configurar la validación de los tokens de enlace de canal configurando el atributo "**tokenChecking**" a un mínimo de "**Allow**" (preferentemente "**Require**") como se documenta en la siguiente guía: Extended Protection for Windows authentication.
- Para LDAP, en la política de grupo se debe establecer que el servidor LDAP requiera necesariamente que los clientes negocien conexiones de datos firmadas, a menos que se esté utilizando TLS/SSL (**"Domain controller: LDAP server signing requirements - Required**"). Esto implica que los dispositivos clientes también deben ser configurados para establecer conexiones firmadas. Puede ver la siguiente guía: LDAP server signing requirements.
- Configurar el la política de grupo "**Domain controller: LDAP server channel binding token requirements" (**Requisitos de token de enlace del canal del servidor LDAP) mínimamente a "When Supported" (Cuándo sea compatible), o preferentemente a "Always" (Siempre) como se documenta en la siguiente guía: LDAP channel binding and LDAP signing requirements for Windows.
- Para SMB, debe configurar la Firma SMB (**SMB Signing**) estableciendo la Política de grupo para firmar digitalmente la comunicación del servidor siempre (**"Digitally sign server communication (always)"**) como se documenta en la siguiente guía: Server Message Block signing.

3. Abuso de los servicios de certificados de Active Directory (ADCS - ESC8):

Las mitigaciones son similares a las descritas para la técnica PetitPotam. Los administradores pueden enumerar las interfaces de enrolamiento web habilitadas en su entorno (por ejemplo, con PSPKIAudit) y ya sea eliminarlas en caso de que no sean utilizadas, o deshabilitar autenticación NTLM en ellas. En caso de que no sea posible deshabilitar NTLM, una posible mitigación es forzar HTTPS en ellas y habilitar Extended Protection for Authentication (EPA) en el componente del servidor IIS.

Puede encontrar instrucciones en la siguiente guía, en la sección "Defensive

Guidance — Harden AD CS HTTP Endpoints — PREVENT8" .

Además, se recomienda a las organizaciones que utilizan el rol AD CS auditar su arquitectura y las plantillas de certificados y tratar a los servidores CA (Certification Authority - Autoridad Certificadora), así como los CAs de nivel inferior como activos críticos con los mismos niveles de protección que un controlador de dominio.

4. PrintNightmare:

Se debe tener en cuenta que, además de instalar el parche, se debe confirmar que los siguiente registros están configurados con el valor 0 (cero) o "No definido".

addition to installing the updates, in order to secure your system, you must confirm that the following registry settings are set to 0 (zero) or are not defined (**Note**: These registry keys do not exist by default, and therefore are already at the secure setting.), also that your Group Policy setting are correct (see FAQ):

- *HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint*
  - *NoWarningNoElevationOnInstall = 0 (DWORD) o no definido (por defecto)*
  - *UpdatePromptSettings = 0 (DWORD) o no definido (por defecto)*

Para más información acerca de medidas de mitigación adicionales y condiciones específicas de su arquitectura, revise el boletín especial del CVE-2021-34527 : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527 (ver sección FAQ)

Como la vulnerabilidad CVE-2021-36958 no tiene todavía parche, la única mitigación posible es deshabilitar temporalmente el servicio. Puede deshabilitar el servicio con los siguientes comandos de Poweshell:

```
Stop-Service -Name Spooler -Force
Set-Service -Name Spooler -StartupType Disabled
```

Tenga en cuenta que parar y deshabilitar el servicio Print Spooner evitará que se pueda imprimir, tanto local como remotamente.

5. SeriousSAM:

Además de instalar el parche, se debe eliminar manualmente todas las Shadow Copies del sistema de archivos, incluida la base de datos SAM. El parche, por sí solo, no corrige el problema. Para eliminarlo, puede seguir la siguiente guía: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934

Otra mitigación temporal posible, en caso de que no se instale el parche, es restringir el acceso al contenido de %windir%\system32\config. Como administrador,

ejecute alguna de las siguientes acciones:

- En el Command Prompt: `icacls %windir%\system32\config\*.* /inheritance:e`
- En Windows PowerShell: `icacls $env:windir\system32\config\*.* /inheritance:e`

En caso de optar por la mitigación, igualmente debe eliminar los Shadow Copies para evitar el riesgo.

Información adicional:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36942
- https://msrc.microsoft.com/update-guide/vulnerability/ADV210003
- https://labs.sentinelone.com/relaying-potatoes-dce-rpc-ntlm-relay-eop/
- https://posts.specterops.io/certified-pre-owned-d95910965cd2
- https://thehackernews.com/2021/08/microsoft-releases-windows-updates-to.html
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934