Los investigadores en ciberseguridad han identificado una vulnerabilidad en el protocolo de autenticación de red RADIUS denominada BlastRADIUS. Esta vulnerabilidad podría ser utilizada por un atacante para realizar ataques de intermediario (MitM) y eludir verificaciones de integridad en determinadas circunstancias.

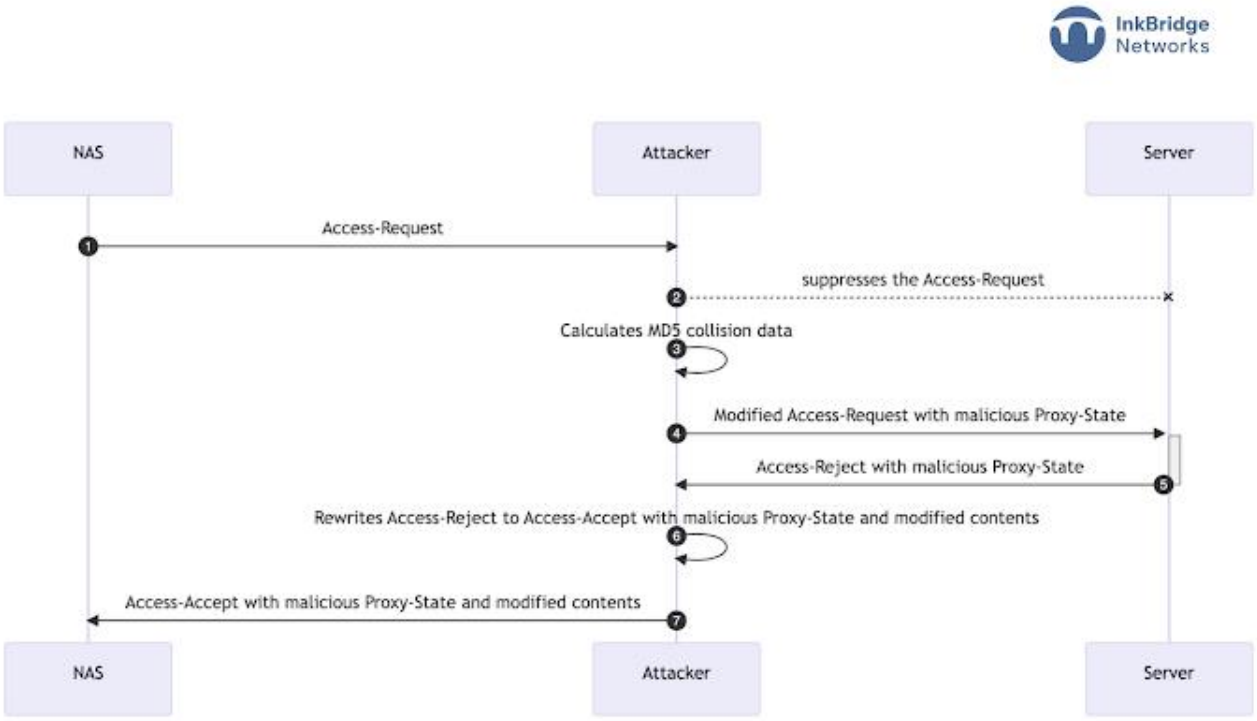
> *«El protocolo RADIUS permite que ciertos mensajes de Solicitud de Acceso no tengan verificaciones de integridad o autenticación»,* dijo en un comunicado Alan DeKok, CEO de InkBridge Networks y creador del Proyecto FreeRADIUS.
>
> *«Como consecuencia, un atacante puede modificar estos paquetes sin ser detectado. El atacante podría obligar a cualquier usuario a autenticarse y otorgarle cualquier autorización (VLAN, etc.) a ese usuario».*

RADIUS, que significa Remote Authentication Dial-In User Service, es un protocolo cliente/servidor que proporciona gestión centralizada de autenticación, autorización y contabilidad (AAA) para los usuarios que se conectan y utilizan un servicio de red.

La seguridad de RADIUS se basa en un hash derivado del algoritmo MD5, que ha sido considerado criptográficamente inseguro desde diciembre de 2008 debido al riesgo de ataques de colisión.

Esto implica que los paquetes de Solicitud de Acceso pueden estar sujetos a un ataque de prefijo elegido, lo que permite modificar el paquete de respuesta de manera que pase todas las verificaciones de integridad del paquete de respuesta original.

Sin embargo, para que el ataque sea exitoso, el atacante debe poder modificar los paquetes RADIUS mientras están en tránsito entre el cliente y el servidor. Esto también significa que las organizaciones que envían paquetes a través de internet están en riesgo debido a esta vulnerabilidad.



Sequence diagram illustrating the attack.

Otros factores de mitigación que previenen que el ataque sea efectivo incluyen el uso de TLS para transmitir tráfico RADIUS a través de internet y una mayor seguridad de los paquetes mediante el atributo Message-Authenticator.

BlastRADIUS es el resultado de una falla de diseño fundamental y se dice que afecta a todos los clientes y servidores RADIUS que cumplen con los estándares, por lo que es imperativo que los proveedores de servicios de internet (ISPs) y las organizaciones que utilizan el protocolo actualicen a la última versión.

> *«Específicamente, los métodos de autenticación PAP, CHAP y MS-CHAPv2 son los más vulnerables. Los ISPs tendrán que actualizar sus servidores RADIUS y equipos de red»*, dijo DeKok.

> *«Cualquiera que use autenticación de direcciones MAC o RADIUS para inicios de sesión de administrador en conmutadores es vulnerable. Usar TLS o IPSec previene el ataque, y 802.1X (EAP) no es vulnerable».*

Para las empresas, el atacante ya necesitaría tener acceso a la red de área local virtual de gestión (VLAN). Además, los ISPs pueden ser vulnerables si envían tráfico RADIUS a través de redes intermedias, como terceros subcontratistas, o la internet más amplia.

Es importante señalar que la vulnerabilidad, identificada como CVE-2024-3596 y con una puntuación CVSS de 9.0, afecta especialmente a las redes que envían tráfico RADIUS/UDP a través de internet dado que *«la mayor parte del tráfico RADIUS se envía 'sin cifrar'».* No hay evidencia de que esté siendo explotada en el mundo real.

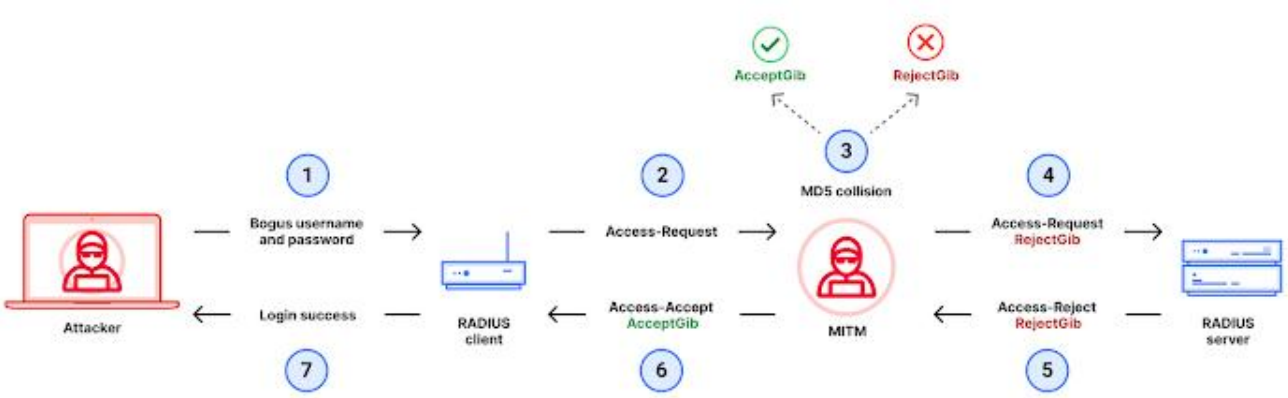
> *«Este ataque es consecuencia de que la seguridad del protocolo RADIUS ha sido descuidada durante mucho tiempo»,* dijo DeKok.
>
> *«Aunque los estándares han recomendado durante mucho tiempo protecciones que habrían evitado el ataque, esas protecciones no se hicieron obligatorias. Además, muchos proveedores ni siquiera implementaron las protecciones sugeridas.»*

Actualización

El Centro de Coordinación CERT (CERT/CC), en un aviso coordinado, describió la vulnerabilidad como una que permite a un atacante con acceso a la red donde se transporta la Solicitud de Acceso RADIUS llevar a cabo ataques de falsificación.

> *«Una vulnerabilidad en el protocolo RADIUS permite a un atacante falsificar una respuesta de autenticación en casos donde no se requiere o aplica un atributo de Message-Authenticator. Esta vulnerabilidad resulta de una verificación de integridad*

> *criptográficamente insegura al validar respuestas de autenticación de un servidor RADIUS»,* dijo CERT/CC.



La empresa de infraestructura web y seguridad Cloudflare ha publicado detalles técnicos adicionales sobre CVE-2024-3596, afirmando que RADIUS/UDP es vulnerable a un ataque mejorado de colisión de MD5.

> *«El ataque permite a un Monstruo-en-el-Medio (MitM) con acceso al tráfico RADIUS obtener acceso administrativo no autorizado a dispositivos que utilizan RADIUS para la autenticación, sin necesidad de forzar contraseñas o robar contraseñas o secretos compartidos»,* indicó.