Un investigador de seguridad cibernética de Tenable, descubrió distintas vulnerabilidades de seguridad en los enrutadores WiFi de Verizon Fios Quantum Gateway, que podrían permitir a los atacantes remotos tomar el control completo de los enrutadores afectados, exponiendo cada uno de los otros dispositivos conectados estos.

Actualmente, millones de consumidores en Estados Unidos, se han visto afectados por las vulnerabilidades de WiFi de Verizon Fios Quantum Gateway, que actualmente son tres vulnerabilidades, identificadas como CVE-2019-3914, CVE-2019-3915 y CVE-2019-3916.

Estas vulnerabilidades son autenticadas con inyección de comandos (con privilegios de root), el inicio de sesión y la revelación de contraseñas en el enrutador de Verizon Fios Quantum Gateway (G1100), según los detalles técnicos de Chris Lyne, un ingeniero de investigación Senior en Tenable.

Fallo de inyección de comando autenticado (CVE-2019-3914)

Al revisar el archivo de registro en su enrutador, Chris notó que las reglas de *«Control de acceso»* en la configuración del Firewall, disponibles en la interfaz web del enrutador, no estaban limpiando correctamente el parámetro *«nombre de host»* al pasar los valores como parte de un comando en la consola.

Entonces, descubrió que al inyectar una entrada maliciosa como nombre de host puede manipular el comando del Firewall, lo que eventualmente permite que un atacante ejecute un código arbitrario en el dispositivo afectado.

> *«Observe que se está emitiendo el comando iptables. Claramente, debo haber ingresado en algún punto. Eso me hizo pensar… Me pregunto si puedo inyectar un comando del sistema operativo en esto. Claramente, esto tiene que ver con las reglas de control de acceso en la configuración del cortafuegos. Investigué la interfaz web para ver si podía encontrarla en algún lugar»,* dijo el investigador en una publicación.

Sin embargo, se debe tener en cuenta que para aprovechar esta vulnerabilidad (CVE-2019-3914), el atacante primero debe acceder a la interfaz web del enrutador, lo que a su vez reduce la superficie de ataque a menos que las víctimas no confíen en las contraseñas predeterminadas.

Además, los enrutadores afectados no vienen con la administración remota habilitada de forma predeterminada, lo que reduce aún más la amenaza de ataques basados en Internet.

> *«Hay dos escenarios de ataque que permiten a un atacante ejecutar comandos de forma remota. Primero, la amenaza interna permitiría a un atacante grabar la secuencia de inicio de sesión utilizando un rastreador de paquetes. Ya sea a través del acceso legítimo o ingeniería social, un atacante podría obtener la contraseña de administrador del enrutador de destino de la etiqueta en el enrutador y la dirección IP pública. Luego, puede activar la administración remota, confirmar que está habilitada o usar la misma maniobra de ingeniería social para que la misma víctima lo habilite»,* dijo Chris a The Hacker News.
>
> *«Después, el atacante puede explotar el CVE-2019-3914 de forma remota, desde todo el Internet, para obtener acceso remoto a la shell raíz del sistema operativo subyacente del enrutador. Desde aquí, tienen el control de la red. Pueden crear puertas traseras, sensibles a los registros. Transacciones por Internet, pivote hacia otros dispositivos, etc.»,* agregó.

Como se muestra en el video de demostración, debido a que el enrutador de Verizon también es compatible con Java debido a la JVM integrada (Java Virtual Machine), un atacante puede simplemente cargar un elemento de pago basado en Java para obtener un shell inverso con privilegios de raíz para lanzar más ataques.

Para ejecutar una shell inversa de Java, el atacante solo necesita cargar y ejecutar una clase de Java, como dijo el investigador, *«logré esto programando al oyente HTTP para que*

devuelva una clase de Java compilada y codificada en Base64 en el cuerpo de la respuesta. Además, el código de Java se compiló para la JVM de destino».

Además de los detalles mostrados en el video, el investigador también publicó el código de vulnerabilidad de prueba de concepto para dicha vulnerabilidad.

La segunda vulnerabilidad, identificada como CVE-2019-3915, existe porque la interfaz de administración web del enrutador se basa en la conexión HTTP insegura.

Permite a los atacantes basados en la red interceptar solicitudes de inicio de sesión utilizando un rastreador de paquetes y reproducirlos para obtener acceso de administrador a la interfaz web.

La tercera vulnerabilidad, identificada como CVE-2019-3916, permite que un atacante no autenticado recupere el valor de la contraseña simplemente visitando una URL en un navegador web.

Debido a que el firmware del enrutador no impone HTTPS, es posible que los atacantes capturen una solicitud de inicio de sesión que contenga el hash de contraseña (SHA-512), que luego se puede utilizar para recuperar la contraseña de texto sin formato.

Tenable reportó las vulnerabilidades a Verizon, mismo que reconoció los problemas y los abordó en una nueva actualización de firmware 02.02.00.13, que se aplicará de forma automática.

> *«Sin embargo, desde Verizon han informado que aún están trabajando para enviar actualizaciones automáticas a una pequeña fracción de los dispositivos. Se recomienda a los usuarios que confirmen que su enrutador está actualizado a la versión 02.02.00.13, y si no es así, comuníquese con Verizon para más información»*.

Una prueba reciente demostró que al menos 15,000 enrutadores WiFi Gateway con administración remota de Verizon Fios Quantum son vulnerables, pero no se sabe cuántos de ellos ejecutan la versión de firmware parcheada.