Investigadores de seguridad cibernética detallaron las vulnerabilidades de seguridad críticas que afectan a los routers de la serie NETGEAR DGN2200v1, mismas que se podrían abusar confiablemente como un punto de partida para comprometer la seguridad de una red y obtener acceso sin restricciones.

Las tres vulnerabilidades de seguridad de autenticación HTTPd, con puntaje CVSS de 7.1-9.4, afectan a los enrutadores que ejecutan versiones de firmware anteriores a la v1.0.0.60, y desde entonces, la compañía las corrigió en diciembre de 2020 como parte de un proceso coordinado de divulgación de vulnerabilidades.

> *«El creciente número de ataques de firmware y ataques de ransomware a través de dispositivos VPN y otros sistemas conectados a Internet son ejemplos de ataques iniciados fuera y debajo de la capa del sistema operativo. A medida que estos tipos de ataques se vuelven más comunes, los usuarios deben buscar proteger incluso el software de un solo propósito que ejecuta su hardware, como los enrutadores»*, dijo Jonathan Bar Or, del equipo de investigación de Microsoft 365 Defender.

Dicho de otra forma las fallas permiten acceder a las páginas de administración en router utilizando un desvío de autenticación, lo que permite a un atacante obtener un control completo sobre le enrutador, así como obtener las credenciales del enrutador guardadas por medio de un ataque de canal lateral criptográfico, e incluso, recuperar el nombre de usuario y contraseña almacenados en la memoria del enrutador mediante la explotación de la función de copia de seguridad/restauración de la configuración.

> *«El nombre de usuario y la contraseña se comparan usando strcmp. La implementación de libc de strcmp funciona comparando caracter por caracter hasta que se observa un terminador NUL o hasta que ocurre una falta de coincidencia. Un atacante podría aprovechar esto último midiendo el tiempo que se tarda en obtener una falla»,* agregó Bar Or.

Además, al abusar de la derivación de autenticación antes mencionada para obtener el archivo de configuración, los investigadores encontraron que las credenciales se cifraron con una clave constante, que se puede utilizar posteriormente para recuperar la contraseña de texto sin formato y el nombre de usuario.

Se recomienda a los usuarios de NETGEAR DGN2200v1 que descarguen y actualicen el firmware al más reciente para evitar posibles ataques.