La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE.UU. (CISA) añadió el jueves dos fallos de seguridad que afectan a los routers D-Link a su catálogo de Vulnerabilidades Conocidas Explotadas (KEV), basándose en pruebas de explotación activa.

Las vulnerabilidades son las siguientes:

- CVE-2014-100005: Una vulnerabilidad de falsificación de solicitud en sitios cruzados (CSRF) que afecta a los routers D-Link DIR-600, permitiendo a un atacante modificar la configuración del router secuestrando una sesión de administrador activa.
- CVE-2021-40655: Una vulnerabilidad de divulgación de información que afecta a los routers D-Link DIR-605, permitiendo a los atacantes obtener un nombre de usuario y una contraseña mediante la falsificación de una solicitud HTTP POST a la página /getcfg.php.

En este momento, no hay detalles sobre cómo se explotan estas vulnerabilidades en el entorno real, pero se ha instado a las agencias federales a aplicar las mitigaciones proporcionadas por el fabricante antes del 6 de junio de 2024.

Es importante señalar que CVE-2014-100005 afecta a productos D-Link antiguos que han llegado al final de su vida útil (EoL), por lo que las organizaciones que todavía los utilizan deben retirarlos y sustituirlos.

Este anuncio llega mientras el equipo de SSD Secure Disclosure ha revelado problemas de seguridad no corregidos en los routers DIR-X4860, que podrían permitir a atacantes remotos no autenticados acceder al puerto HNAP para obtener permisos elevados y ejecutar comandos como superusuario.

> «*Combinando una omisión de autenticación con la ejecución de comandos, el dispositivo puede ser completamente comprometido,*» dijeron, agregando que los problemas afectan a los routers con la versión de firmware DIRX4860A1_FWV1.04B03.

SSD Secure Disclosure también ha publicado un exploit de prueba de concepto (PoC), que emplea una solicitud de inicio de sesión HNAP especialmente diseñada para la interfaz de administración del router con el fin de eludir las protecciones de autenticación y lograr la ejecución de código aprovechando una vulnerabilidad de inyección de comandos.

D-Link ha reconocido el problema en un boletín propio, afirmando que una solución está «Pendiente de Lanzamiento / En Desarrollo.» Describieron la vulnerabilidad como un caso de ejecución de comandos no autenticados desde el lado LAN.

Ivanti Corrige Varias Vulnerabilidades en Endpoint Manager Mobile (EPMM)

Investigadores de ciberseguridad también han lanzado un exploit PoC para una nueva vulnerabilidad en Ivanti EPMM (CVE-2024-22026, puntuación CVSS: 6.7) que podría permitir a un usuario local autenticado eludir la restricción de shell y ejecutar comandos arbitrarios en el dispositivo.

> *«Esta vulnerabilidad permite a un atacante local obtener acceso root al sistema explotando el proceso de actualización de software con un paquete RPM malicioso desde una URL remota,»* dijo Bryan Smith de Redline Cyber Security.

El problema surge de una validación inadecuada en el comando de instalación de la interfaz de línea de comandos de EPMM, que puede descargar un paquete RPM arbitrario desde una URL proporcionada por el usuario sin verificar su autenticidad.

CVE-2024-22026 afecta a todas las versiones de EPMM anteriores a la 12.1.0.0. Ivanti también ha corregido otros dos fallos de inyección SQL en el mismo producto (CVE-2023-46806 y CVE-2023-46807, puntuaciones CVSS: 6.7) que podrían permitir a un usuario autenticado con privilegios adecuados acceder o modificar datos en la base de datos subyacente.

Aunque no hay evidencia de que estas vulnerabilidades hayan sido explotadas, se recomienda a los usuarios actualizar a la última versión para mitigar posibles amenazas.