Investigadores de seguridad cibernética descubrieron ayer los detalles referentes a dos nuevas vulnerabilidades en el software del servidor web GoAhead, una pequeña aplicación ampliamente integrada en cientos de millones de dispositivos inteligentes conectados a Internet.

Una de las dos vulnerabilidades, asignada como CVE-2019-5096, es una falla de ejecución de código crítica que los atacantes pueden explotar para ejecutar código malicioso en dispositivos vulnerables y tomar el control sobre ellos.

La primera vulnerabilidad reside en la forma en que se procesan las solicitudes multiparte/datos de formulario, dentro de la aplicación base del servidor web GoAhead, que afecta a las versiones del servidor web GoAhead v5.0.1, v.4.1.1 y v3.6.5.

Según los investigadores de Cisco Talos, mientras se procesa una solicitud HTTP especialmente diseñada, un atacante que explota la vulnerabilidad puede causar una condición libre de uso en el servidor y estructuras de montón corruptas, lo que lleva a ataques de ejecución de código.

La segunda vulnerabilidad, asignada como CVE-2019-5097, también reside en el mismo componente del servidor web GoAhead y puede explotarse de la misma forma, pero esta conduce a ataques de denegación de servicio.

> *«Una solicitud HTTP especialmente diseñada puede conducir a un bucle infinito en el proceso (resultando en una utilización del 100 por ciento de la CPU). La solicitud no se puede autenticar en forma de solicitudes GET o POST y no requiere que el recurso solicitado exista en el servidor»*, dicen los investigadores.

Sin embargo, no es necesario que ambas vulnerabilidades puedan explotarse en todos los dispositivos integrados que ejecutan las versiones vulnerables del servidor web GoAhead.

Esto es porque, según los investigadores, debido a que GoAhead es un marco de aplicación

web personalizable, las empresas implementan la aplicación de acuerdo con su entorno y requisitos, por lo que los defectos *«pueden no ser accesibles en todas las compilaciones».*

> *«Además, las páginas que requieren autenticación no permiten el acceso a la vulnerabilidad sin autenticación, ya que la autenticación se maneja antes de llegar al controlador de carga».*

Los investigadores de Talos informaron sobre las vulnerabilidades a EmbedThis, el desarrollador de la aplicación GoAhead Web Server, a fines de agosto de este año, y el proveedor abordó los problemas y lanzó parches de seguridad hace dos semanas.