BOLETÍN DE ALERTA

Boletín Nro.: 2017-09
Fecha de publicación: 06/06/2017
Tema: Vulnerabilidad de desbordamiento de buffer en routers Netgear

Sistemas afectados:

- Equipos Netgear:
  - WNR2000v3
  - WNR2000v4
  - WNR2000v5
  - R2000

Descripción:

Se ha descubierto una vulnerabilidad de desbordamiento de buffer en el firmware de varios modelos de equipos de Netgear, la cual permite a un atacante remoto no autenticado la ejecución remota de código arbitrario. La vulnerabilidad ha sido identificada como CVE-2017-6862 y se debe a que no se verifica adecuadamente los límites de tamaño de los datos provistos por el usuario en ciertas condiciones, antes de copiarlos a un buffer de memoria. Explotando esta vulnerabilidad, se puede obtener acceso al panel web de administración.

La vulnerabilidad puede ser explotada si un atacante tiene acceso a la red interna o cuando la administración remota está habilitada en el router.

Netgear ha publicado un firmware actualizado para todos los modelos afectados. Las versiones de firmware que corrigen esta vulnerabilidad son: 1.1.2.14 (WNR2000v3), 1.0.0.66 (WNR2000v4) y 1.0.0.42 (WNR2000v5).

Impacto:

Un cibercriminal puede obtener el control total del router y cambiar la configuración para llevar a cabo otro tipo de ataques que busquen comprometer los equipos de la red.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Solución:

Para obtener la actualización del firmware, debe ingresar al centro de descargas de Netgear: http://downloadcenter.netgear.com/

En el buscador, debe tildar únicamente "Firmware/Software" e ingresar el modelo de su router (Ej.: WNR2000) y seleccionar el modelo adecuado del menú desplegado. Deberá descargar la última versión de firmware disponible. En "Release Notes" podrá obtener instrucciones detalladas de acuerdo al modelo.

Además. se recomienda limitar o desactivar la administración remota en caso de que no sea estrictamente necesario.

Información adicional:

https://kb.netgear.com/000038542/Security-Advisory-for-Unauthenticated-Remote-Code-Execution-on-Some-Routers-PSV-2016-0261

http://www.securityfocus.com/bid/98740/discuss

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py