SECRETARÍA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

BOLETÍN DE ALERTA

Boletín Nro.: 2014-09

Fecha de publicación: 22/12/2014

Tema: Vulnerabilidades en Network Time Protocol daemon (ntpd)

Sistemas afectados:

Versiones de NTP anteriores a la versión 4.2.8, publicada el 19 de diciembre.

Puede ver la lista completa en:

http://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=852879&SearchOrder=4

Descripción:

Network Time Protocol (NTP) es un protocolo que proporciona a los sistemas en red una forma de sincronizar la hora de los diferentes servicios y aplicaciones. Se descubrieron vulnerabilidades de desbordamiento de varios *buffers* en la versión ntpd 4.2.7 y las versiones previas, lo que puede permitir a atacantes la ejecución de código malicioso. Además, el generador de claves ntp (ntp-keygen) previo a la versión 4.2.7p230 utiliza un generador de números aleatorios no criptográfico al generar claves simétricas.

CWE-332: Entropía Insuficiente en PRNG (Generador de Números Pseudo-Randómicos) - CVE-2014-9293

Si no se define una clave de autenticación en el archivo **ntp.conf**, se genera una clave criptográfica predeterminada y débil.

CWE-338: Uso de PRNG criptográficamente débil - CVE-2014-9294
ntp-keygen anterior a 4.2.7p230 utiliza un generador de números aleatorios no criptográfico con un kernel débil, al generar claves simétricas.

CERT-PY Equipo de Respuesta ante Emergencias Cibernéticas (CERT-py)
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

CWE-121: Desbordamiento de Stack Buffer - CVE-2014-9295

Un atacante remoto no autenticado puede enviar paquetes específicos de modo a producir un desbordamiento de *buffer* en las funciones de ntpd: crypto_recv(), ctl_putdata() y configure(). Esto puede ser explotado para permitir la ejecución arbitraria de código malicioso, con los permisos del proceso ntpd.

CWE-389: Condiciones de error, valor de retorno y código de status inesperados - CVE-2014-9296

En una sección del código de ntpd de manejo de errores falta una declaración de retorno, por lo que al procesar cierto tipo de errores, la función no retorna y el procesamiento no se detiene.

Impacto:

Las vulnerabilidades de desbordamiento de *buffer* en ntpd pueden permitir a un atacante remoto no autenticado ejecutar código malicioso arbitrario, con el nivel de privilegios del proceso ntpd. La clave por defecto débil y el generador de números aleatorios no criptográficos en ntp-keygen pueden permitir a un atacante obtener información acerca de la comprobación de integridad y de los esquemas del cifrado de autenticación.

Existen *exploits* públicamente disponibles para la explotación de dichas vulnerabilidades.

Solución:

NTP publicó una actualización que corrige estas vulnerabilidades, ntpd-4.2.8, la cual puede ser descargada de:

http://www.ntp.org/downloads.html

Se recomienda actualizar los sistemas en la brevedad posible.

Información adicional:

http://support.ntp.org/bin/view/Main/SecurityNotice
http://www.ntp.org/ntpfaq/NTP-s-algo-crypt.htm
http://www.kb.cert.org/vuls/id/852879
https://ics-cert.us-cert.gov/advisories/ICSA-14-353-01

CERT-PY Equipo de Respuesta ante Emergencias Cibernéticas (CERT-py)
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