BOLETÍN DE ALERTA

Boletín Nro.: 2023-38
Fecha de publicación: 21/08/2023
Tema: Vulnerabilidades en Junos OS explotadas en conjunto permitirían ejecución remota de código (*RCE*)

Principales productos afectados son:

- Junos OS en SRX Series, todas las versiones anteriores a 20.4R3-S8.
- Junos OS en SRX Series, versión 21.2 y anteriores a 21.2R3-S6.
- Junos OS en SRX Series, versión 21.3 y anteriores a 21.3R3-S5.
- Junos OS en la serie EX, todas las versiones anteriores a 20.4R3-S8.
- Junos OS en la serie EX, versión 21.2 y anteriores a 21.2R3-S6.
- Junos OS en la serie EX, versión 21.3 y anteriores a 21.3R3-S5.

Se puede acceder al listado completo de vulnerabilidades aquí

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre cuatro vulnerabilidades que afectan a Juniper Junos OS, estas vulnerabilidades, cuando se combinan y explotadas en conjunto, podrían permitir que un actor malicioso ejecute código de forma remota (*RCE*) en el sistema afectado.

Las vulnerabilidades corregidas se componen de 4 (cuatro) de severidad “Media. Las mismas se detallan a continuación:

- CVE-2023-36844 y CVE-2023-36845, ambas de severidad “Media” y con puntuación de 5.3. Estas vulnerabilidades se deben a una falla de modificación en las variables externas de *PHP* en la interfaz *J-Web* de los dispositivos Juniper Networks Junos OS en *EX* Series y *SRX* Series. Esto permitiría a un atacante no autenticado a través de una solicitud especialmente diseñada, modificar una determinada variable de entorno *PHP en la interfaz J-Web que* potencialmente podrían derivar en la ejecución remota de código (*RCE*) en el sistema afectado.

- CVE-2023-36846 y CVE-2023-36847, ambas de severidad “Media” y con puntuación de 5.3. Estas vulnerabilidades se deben a una falla de autenticación en funciones críticas de Juniper Networks Junos OS en SRX Series. Esto permitiría a un atacante no autenticado acceder a funciones específicas en el sistema afectado, y a través de ellas realizar la subida de archivos arbitrarios a través de la interfaz *J-Web*.

Impacto:

La explotación exitosa de forma conjunta de estas vulnerabilidades podría permitir a un atacante realizar ejecución remota de código (*RCE*) en el sistema afectado.

Mitigación:

Recomendamos como medida de mitigación temporal considerar realizar el siguiente paso:

- Desactivar el acceso a *J-Web* o limitar el acceso solo para *hosts* de confianza.

Adicionalmente recomendamos estar pendiente a posibles actualizaciones correspondientes y/o parches que se publiquen en el futuro apenas sean provistas por el fabricante en el siguiente enlace:

- https://support.juniper.net/support/downloads/

Información adicional:

- https://thehackernews.com/2023/08/new-juniper-junos-os-flaws-expose.html
- https://vulnera.com/newswire/juniper-networks-patches-critical-flaws-in-switches-and-firewalls/
- https://nvd.nist.gov/vuln/detail/CVE-2023-36844
- https://nvd.nist.gov/vuln/detail/CVE-2023-36845
- https://nvd.nist.gov/vuln/detail/CVE-2023-36846
- https://nvd.nist.gov/vuln/detail/CVE-2023-36847
- https://supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution?language=en_US
- https://support.juniper.net/support/downloads/