

| | |
|---------------------------------|------------------------------|
| Alerta de seguridad cibernética | 9VSA20-00268-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 10 de julio de 2020 |
| Última revisión | 10 de julio de 2020 |

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afectada a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de Juniper respecto a varias vulnerabilidades en sus productos Juniper Networks Junos OS, Juniper Secure Analytics, Junos OS y Junos Space Security Director, que permitirían a un atacante ejecutar código remoto en los sistemas o provocar una condición de denegación de servicio. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

| | | |
|---------------|------------------|---------------|
| CVE-2020-4274 | CVE-2019-4508 | CVE-2015-7940 |
| CVE-2017-3164 | CVE-2019-17359 | CVE-2013-1624 |
| CVE-2020-4294 | CVE-2018-1000613 | CVE-2007-6721 |
| CVE-2019-2989 | CVE-2018-1000180 | CVE-2020-1650 |
| CVE-2019-2975 | CVE-2018-5382 | CVE-2020-1651 |
| CVE-2019-2981 | CVE-2017-13098 | CVE-2020-1649 |
| CVE-2019-2973 | CVE-2016-1000352 | CVE-2020-1648 |
| CVE-2019-2964 | CVE-2016-1000346 | CVE-2020-1647 |
| CVE-2019-4593 | CVE-2016-1000345 | CVE-2020-1646 |
| CVE-2020-4272 | CVE-2016-1000344 | CVE-2020-1644 |
| CVE-2020-4270 | CVE-2016-1000343 | CVE-2020-1654 |
| CVE-2020-4269 | CVE-2016-1000342 | CVE-2020-1641 |
| CVE-2019-4594 | CVE-2016-1000341 | CVE-2020-1645 |
| CVE-2020-4268 | CVE-2016-1000340 | CVE-2020-1640 |
| CVE-2020-4271 | CVE-2016-1000339 | CVE-2020-1643 |
| CVE-2019-4654 | CVE-2016-1000338 | |
| CVE-2018-0734 | CVE-2016-2427 | |

Múltiples vulnerabilidades (1)

CVEs

CVE-2020-4274
CVE-2017-3164
CVE-2020-4294
CVE-2019-2989
CVE-2019-2975
CVE-2019-2981
CVE-2019-2973
CVE-2019-2964
CVE-2019-4593
CVE-2020-4272
CVE-2020-4270
CVE-2020-4269
CVE-2019-4594
CVE-2020-4268
CVE-2020-4271
CVE-2019-4654
CVE-2018-0734
CVE-2019-4508

Problema

Se han resuelto múltiples vulnerabilidades en Juniper Secure Analytics (JSA) JSA 7.3.2 parche 7, 7.3.3 parche 3 y 7.4.0 mediante la reparación de vulnerabilidades en los paquetes de software de terceros además de otros componentes de software. Juniper SIRT no tiene conocimiento de ninguna explotación maliciosa de estas vulnerabilidades.

Productos afectados

Juniper Networks Juniper Secure Analytics (JSA), versiones

- 7.3.0
- 7.3.1
- 7.3.2 versiones anteriores a 7.3.2 Patch 7
- 7.3.3 versiones anteriores a 7.3.3 Patch 3

Mitigación

Los problemas enumerados anteriormente se han resuelto en JSA: 7.3.2 parche 7, 7.3.3 parche 3, 7.4.0 y todas las versiones posteriores.

Enlace

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11042&cat=SIRT_1&actp=LIST

Múltiples vulnerabilidades (2)

CVEs

CVE-2019-17359
CVE-2018-1000613
CVE-2018-1000180
CVE-2018-5382
CVE-2017-13098
CVE-2016-1000352
CVE-2016-1000346
CVE-2016-1000345
CVE-2016-1000344
CVE-2016-1000343
CVE-2016-1000342
CVE-2016-1000341
CVE-2016-1000340
CVE-2016-1000339
CVE-2016-1000338
CVE-2016-2427
CVE-2015-7940
CVE-2013-1624
CVE-2007-6721

Problema

Se han solucionado múltiples vulnerabilidades en el software de Control de sesión y recursos (SRC) actualizando el paquete Bouncy Castle a la versión 1.62.

Productos afectados

SRC de Juniper Networks, versiones

- 4.12.0 versiones anteriores a 4.12.0-R4;
- 4.13.0 versiones anteriores a 4.13.0-R2.

Mitigación

Las siguientes versiones de software se han actualizado para resolver este problema específico: SRC 4.12.0-R4, 4.13.0-R2 y todas las versiones posteriores.

Enlaces:

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11039&cat=SIRT_1&actp=LIST

CVE-2020-1655

Problema

Cuando un dispositivo que ejecuta Juniper Networks Junos OS con tarjetas de línea MPC7, MPC8 o MPC9 instaladas y el sistema está configurado para el reensamblado de IP en línea, utilizado por L2TP, MAP-E, GRE e IPIP, el motor de reenvío de paquetes (PFE) se convertirá deshabilitado al recibir paquetes grandes que requieren fragmentación, generando un mensaje de error.

Productos afectados

Este problema afecta a Junos OS 17.2, 17.3, 17.4, 18.1, 18.2, 18.2X75, 18.3, 18.4, 19.1, 19.2, 19.3. Plataformas afectadas: Serie MX.

Mitigación

Las siguientes versiones de software se han actualizado para resolver este problema específico: Junos OS 17.2R3-S4, 17.3R3-S8, 17.4R2-S10, 17.4R3-S2, 18.1R3-S10, 18.2R3-S3, 18.2X75-D41, 18.2X75-D430, 18.2X75-D65, 18.3R1-S7, 18.3R2-S4, 18.3R3-S1, 18.4R1-S7, 18.4R2-S4, 18.4R3, 19.1R1-S5, 19.1R2-S1, 19.1R3, 19.2R1-S4, 19.2R2, 19.3R2-S2, 19.3R3, 19.4R1, 19.4R2, 20.1R1 y todas las versiones posteriores.

Enlaces:

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11041&cat=SIRT_1&actp=LIST

CVE-2020-1653

Problema

En los dispositivos de Juniper Networks Junos OS, una secuencia de paquetes TCP enviados al Motor de enrutamiento (RE) puede causar una fuga de mbuf que puede provocar un bloqueo del Concentrador PIC flexible (FPC) o el sistema se bloquea y reinicia (vmcore). Este problema puede ser desencadenado por IPv4 o IPv6 y solo es causado por paquetes TCP. Este problema no está relacionado con ninguna configuración específica y afecta a las versiones del sistema operativo Junos a partir de 17.4R1. Sin embargo, este problema no afecta a las versiones del sistema operativo Junos anteriores a 18.2R1 cuando se configura el enrutamiento activo sin interrupciones (NSR).

Productos afectados

Este problema afecta a Junos OS 17.4, 18.1, 18.2, 18.2X75, 18.3, 18.4, 19.1, 19.2, 19.3, 19.4.

Mitigación

Las siguientes versiones se han actualizado para resolver este problema: 17.4R2-S11, 17.4R3-S2, 18.1R3-S10, 18.2R2-S7, 18.2R3-S5, 18.2X75-D41, 18.2X75-D420.12, 18.2X75-D51, 18.2X75-D60, 18.2X75-D34, 18.3R2-S4, 18.3R3-S2, 18.4R1-S7, 18.4R2-S4, 18.4R3-S1, 19.1R1-S5, 19.1R2-S1, 19.1R3, 19.2R1-S5, 19.2R2, 19.3R2-S3, 19.3R3, 19.4R1-S2, 19.4R2, 20.1R1 y todas las versiones posteriores.

Enlaces:

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11041&cat=SIRT_1&actp=LIST

CVE-2020-1650

Problema

En Juniper Networks Junos MX Series con tarjeta de servicio configurada, la recepción de una secuencia de paquetes específicos puede bloquear el componente MS-PIC en MS-MIC o MS-MPC. Al enviar continuamente estos paquetes específicos, un atacante puede derribar repetidamente MS-PIC en MS-MIC / MS-MPC causando una Denegación de Servicio prolongada..

Productos afectados

Este problema afecta a los dispositivos de la serie MX que utilizan tarjetas de servicio MS-PIC, MS-MIC o MS-MPC con cualquier servicio configurado

Juniper Networks Junos OS en la serie MX:

- 17.2R2-S7;
- 17.3R3-S4, 17.3R3-S5;
- 17.4R2-S4 y los SR posteriores (17.4R2-S5, 17.4R2-S6, etc.);
- 17.4R3;
- 18.1R3-S3, 18.1R3-S4, 18.1R3-S5, 18.1R3-S6, 18.1R3-S7, 18.1R3-S8;
- 18.2R3, 18.2R3-S1, 18.2R3-S2;
- 18.3R2 y los SR basados en 18.3R2;
- 18.4R2 y los SR basados en 18.4R2;
- 19.1R1 y los SR basados en 19.1R1;
- 19.2R1 y los SR basados en 19.2R1;
- 19.3R1 y los SR basados en 19.3R1.

Mitigación

Las siguientes versiones de software se han actualizado para resolver este problema específico: 17.2R2-S8, 17.3R3-S6, 17.4R3-S1, 18.1R3-S9, 18.2R3-S3, 18.3R3, 18.4R3, 19.1R2, 19.2R2, 19.3R2, 19.4R1 y todas las versiones posteriores.

Enlaces:

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11037&cat=SIRT_1&actp=LIST

CVE-2020-1651

Problema

En la serie MX de Juniper Networks, la recepción de un flujo de tramas específicas de la Capa 2 puede causar una pérdida de memoria que ocasiona que el motor de reenvío de paquetes (PFE) en la tarjeta de línea se bloquee y reinicie, causando interrupción del tráfico.

Al enviar continuamente este flujo de trama específica de capa 2, un atacante conectado al mismo dominio de difusión puede bloquear repetidamente el PFE, causando una Denegación de Servicio (DoS) prolongada.

Productos afectados

Este problema afecta a Junos OS 17.2, 17.2X75, 17.3, 17.4, 18.1. Plataformas afectadas: Serie MX.

Juniper Networks Junos OS en la serie MX17.2R2-S7;

- 17.2 versiones anteriores a 17.2R3-S4;
- 17.2X75 versiones anteriores a 17.2X75-D105.19;
- 17.3 versiones anteriores a 17.3R3-S7;
- 17.4 versiones anteriores a 17.4R1-S3, 17.4R2;
- 18.1 versiones anteriores a 18.1R2.

Mitigación

Las siguientes versiones de software se han actualizado para resolver este problema específico: 17.2R3-S4, 17.2X75-D105.19, 17.3R3-S7, 17.4R1-S3, 17.4R2, 18.1R2, 18.2R1, 18.2X75-D10 y Todos los lanzamientos posteriores.

Enlaces:

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11038&cat=SIRT_1&actp=LIST

CVE-2020-1649

Problema

Cuando un dispositivo que ejecuta Juniper Networks Junos OS con tarjetas de línea MPC7, MPC8 o MPC9 instaladas y el sistema está configurado para el reensamblado de IP en línea, utilizado por L2TP, MAP-E, GRE e IPIP, el motor de reenvío de paquetes (PFE) se convertirá deshabilitado al recibir fragmentos pequeños que requieren reensamblaje, generando un mensaje de error.

Productos afectados

Este problema afecta a Junos OS 17.2, 17.3, 17.4, 18.1, 18.2, 18.2X75, 18.3, 18.4, 19.1, 19.2, 19.3. Plataformas afectadas: Serie MX.

Juniper Networks Junos OS

- 17.2 versiones anteriores a 17.2R3-S4 en la serie MX;
- 17.3 versiones anteriores a 17.3R3-S8 en la serie MX;
- 17.4 versiones anteriores a 17.4R2-S9, 17.4R3-S1 en la serie MX;
- Versiones 18.1 anteriores a 18.1R3-S10 en la serie MX;
- 18.2 versiones anteriores a 18.2R2-S6, 18.2R3-S3 en la serie MX;
- Versiones 18.2X75 anteriores a 18.2X75-D34, 18.2X75-D41, 18.2X75-D53, 18.2X75-D65, 18.2X75-D430 en la serie MX;
- Versiones 18.3 anteriores a 18.3R1-S7, 18.3R2-S4, 18.3R3-S2 en la serie MX;
- Versiones 18.4 anteriores a 18.4R1-S6, 18.4R2-S4, 18.4R3 en la serie MX;
- 19.1 versiones anteriores a 19.1R1-S4, 19.1R2-S1, 19.1R3 en la serie MX;
- 19.2 versiones anteriores a 19.2R1-S3, 19.2R2 en la serie MX;
- 19.3 versiones anteriores a 19.3R2-S2, 19.3R3 en la serie MX..

Mitigación

Las siguientes versiones se han actualizado para resolver este problema específico: Junos OS 17.2R3-S4, 17.3R3-S8, 17.4R2-S9, 17.4R3-S1, 18.1R3-S10, 18.2R2-S6, 18.2R3-S3, 18.2X75-D34, 18.2X75-D41, 18.2X75-D53, 18.2X75-D65, 18.2X75-D430, 18.3R1-S7, 18.3R2-S4, 18.3R3-S2, 18.4R1-S6, 18.4R2-S4, 18.4R3, 19.1R1-S4, 19.1R2-S1, 19.1R3, 19.2R1-S3, 19.2R2, 19.3R2-S2, 19.3R3, 19.4R1, 19.4R2, 20.1R1, y todas las versiones posteriores.

Enlaces:

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11036&cat=SIRT_1&act=LIST

CVE-2020-1647

Problema

En la serie SRX de Juniper Networks con el servicio de redireccionamiento ICAP (Protocolo de adaptación de contenido de Internet) habilitado, una doble vulnerabilidad libre puede conducir a una Denegación de servicio (DoS) o Ejecución remota de código (RCE) debido al procesamiento de un mensaje HTTP específico. El procesamiento continuo de este mensaje HTTP específico puede resultar en una Denegación de Servicio (DoS) extendida. El mensaje HTTP ofensivo que causa este problema puede originarse tanto en el servidor HTTP como en el cliente.

Productos afectados

Este problema afecta a Junos OS 18.2X75, 19.4, 20.1. Este problema afecta a Junos OS Evolved 19.4-EVO, 20.1-EVO.

Juniper Networks Junos OS en la serie SRX

- 18.1 versiones anteriores a 18.1R3-S9;
- 18.2 versiones anteriores a 18.2R3-S3;
- 18.3 versiones anteriores a 18.3R2-S4, 18.3R3-S1;
- 18.4 versiones anteriores a 18.4R2-S5, 18.4R3;
- 19.1 versiones anteriores a 19.1R2;
- 19.2 versiones anteriores a 19.2R1-S2, 19.2R2;
- 19.3 versiones anteriores a 19.3R2.

Mitigación

Las siguientes versiones de software se han actualizado para resolver este problema específico: 18.1R3-S9, 18.2R3-S3, 18.3R2-S4, 18.3R3-S1, 18.4R2-S5, 18.4R3, 19.1R2, 19.2R1-S2, 19.2R2, 19.3R2, 19.4R1 y todas las versiones posteriores.

Enlaces:

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11034&cat=SIRT_1&actp=LIST

CVE-2020-1646

Problema

En los dispositivos Juniper Networks Junos OS y Junos OS Evolved, el procesamiento de una actualización específica para un par EBGP puede provocar un bloqueo y reinicio del demonio del proceso de enrutamiento (RPD). Este problema ocurre solo cuando el dispositivo está recibiendo y procesando la actualización BGP para un par EBGP. Este problema no ocurre cuando el dispositivo recibe y procesa la actualización BGP para un par IBGP. Sin embargo, la actualización BGP ofensiva puede provenir originalmente de un par EBGP, se propaga a través de la red a través de pares IBGP sin causar un bloqueo, luego causa un bloqueo RPD cuando se procesa para una actualización BGP hacia un par EBGP. La recepción y el procesamiento repetidos de la misma actualización BGP específica pueden resultar en una condición extendida de Denegación de Servicio (DoS).

Productos afectados

Este problema afecta a Junos OS 17.3, 17.4, 18.1. Este problema afecta a Junos OS Evolved 19.2-EVO.

Juniper Networks Junos OS en la serie SRX

- 18.1 versiones anteriores a 18.1R3-S9;
- 18.2 versiones anteriores a 18.2R3-S3;
- 18.3 versiones anteriores a 18.3R2-S4, 18.3R3-S1;
- 18.4 versiones anteriores a 18.4R2-S5, 18.4R3;
- 19.1 versiones anteriores a 19.1R2;
- 19.2 versiones anteriores a 19.2R1-S2, 19.2R2;
- 19.3 versiones anteriores a 19.3R2.

Mitigación

Las siguientes versiones de software se han actualizado para resolver este problema específico:

- Sistema operativo Junos: 17.3R3-S7, 17.4R2-S8, 18.1R3-S8 y todas las versiones posteriores.
- Junos OS Evolved: 19.3R1-EVO y todas las versiones posteriores

Enlaces:

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11033&cat=SIRT_1&actp=LIST

CVE-2020-1648

Problema

En los dispositivos Juniper Networks Junos OS y Junos OS Evolved, el procesamiento de un paquete BGP específico puede provocar un bloqueo y reinicio del demonio del proceso de enrutamiento (RPD). Este problema puede ocurrir incluso antes de que se establezca la sesión BGP con el igual. La recepción repetida de este paquete BGP específico puede resultar en una condición extendida de Denegación de Servicio (DoS).

Productos afectados

Este problema afecta a Junos OS 18.2X75, 19.4, 20.1. Este problema afecta a Junos OS Evolved 19.4-EVO, 20.1-EVO.

Juniper Networks Junos OS

- Versiones 18.2X75 a partir de 18.2X75-D50.8, 18.2X75-D60 y versiones posteriores, anteriores a 18.2X75-D52.8, 18.2X75-D53, 18.2X75-D60.2, 18.2X75-D65.1, 18.2X75 -D70;
- 19.4 versiones 19.4R1 y 19.4R1-S1;
- 20.1 versiones anteriores a 20.1R1-S2, 20.1R2.

Juniper Networks Junos OS Evolucionado

- 19.4-EVO versiones anteriores a 19.4R2-S2-EVO;
- Versiones 20.1-EVO anteriores a 20.1R2-EVO.

Mitigación

Las siguientes versiones de software se han actualizado para resolver este problema específico:
Sistema operativo Junos: 18.2X75-D52.8, 18.2X75-D53, 18.2X75-D60.2, 18.2X75-D65.1, 18.2X75-D70, 19.4R1-S2, 19.4R2, 20.1R1-S2, 20.1R2, 20.2R1, y todas las versiones posteriores.
Junos OS Evolved: 19.4R2-S2-EVO, 20.1R2-EVO, 20.2R1-EVO y todas las versiones posteriores.

Enlaces:

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11035&cat=SIRT_1&actp=LIST

CVE-2020-1644

Problema

En los dispositivos Juniper Networks Junos OS y Junos OS Evolved, la recepción de un paquete específico de ACTUALIZACIÓN BGP hace que un contador interno se incremente incorrectamente, lo que con el tiempo puede provocar el bloqueo y el reinicio del proceso de protocolos de enrutamiento (RPD). Este problema afecta a la implementación de múltiples tiendas IBGP y EBGP en redes IPv4 o IPv6.

Productos afectados

Este problema afecta a Junos OS 17.2X75, 17.3, 17.4, 18.1, 18.2, 18.2X75, 18.3, 18.4, 19.1, 19.2, 19.3, 19.4. Este problema afecta a Junos OS Evolved 19.2-EVO, 19.3-EVO, 19.4-EVO, 20.1-EVO.

Juniper Networks Junos OS

- 17.2X75 versiones anteriores a 17.2X75-D105.19;
- 17.3 versiones anteriores a 17.3R3-S8;
- 17.4 versiones anteriores a 17.4R2-S10, 17.4R3-S2;
- 18.1 versiones anteriores a 18.1R3-S10;
- 18.2 versiones anteriores a 18.2R2-S7, 18.2R3-S4;
- Versiones 18.2X75 anteriores a 18.2X75-D13, 18.2X75-D411.1, 18.2X75-D420.18, 18.2X75-D52.3, 18.2X75-D60;
- 18.3 versiones anteriores a 18.3R2-S4, 18.3R3-S2;
- 18.4 versiones anteriores a 18.4R1-S7, 18.4R2-S4, 18.4R3-S2;
- 19.1 versiones anteriores a 19.1R1-S5, 19.1R2-S1, 19.1R3;
- 19.2 versiones anteriores a 19.2R1-S5, 19.2R2;
- 19.3 versiones anteriores a 19.3R2-S2, 19.3R3;
- 19.4 versiones anteriores a 19.4R1-S2, 19.4R2.

Mitigación

Las siguientes versiones de software se han actualizado para resolver este problema específico:

- Sistema operativo Junos: 17.2X75-D105.19, 17.3R3-S8, 17.4R2-S10, 17.4R3-S2, 18.1R3-S10, 18.2R2-S7, 18.2R3-S4, 18.2X75-D13, 18.2X75-D411. 1, 18.2X75-D420.18, 18.2X75-D52.3, 18.2X75-D60, 18.3R2-S4, 18.3R3-S2, 18.4R1-S7, 18.4R2-S4, 18.4R3-S2, 19.1R1-S5, 19.1R2-S1, 19.1R3, 19.2R1-S5, 19.2R2, 19.3R2-S2, 19.3R3, 19.4R1-S2, 19.4R2, 20.1R1 y todas las versiones posteriores.
- Junos OS Evolved: 20.1R2-EVO, 20.2R1-EVO y todas las versiones posteriores.

Enlaces:

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11032&cat=SIRT_1&actp=LIST

CVE-2020-1654

Problema

En la serie SRX de Juniper Networks con el servicio de redireccionamiento ICAP (Protocolo de adaptación de contenido de Internet) habilitado, el procesamiento de un mensaje HTTP con formato incorrecto puede provocar una Denegación de servicio (DoS) o Ejecución remota de código (RCE). El procesamiento continuo de este mensaje HTTP con formato incorrecto puede generar una condición de denegación de servicio (DoS) extendida. El mensaje HTTP ofensivo que causa este problema puede originarse tanto en el servidor HTTP como en el cliente HTTP.

Productos afectados

Este problema afecta a Junos OS 18.1, 18.2, 18.3, 18.4, 19.1, 19.2, 19.3. Plataformas afectadas: Serie SRX.

Juniper Networks Junos OS en la serie SRX

- 18.1 versiones anteriores a 18.1R3-S9;
- 18.2 versiones anteriores a 18.2R2-S7, 18.2R3-S3;
- 18.3 versiones anteriores a 18.3R1-S7, 18.3R2-S4, 18.3R3-S1;
- 18.4 versiones anteriores a 18.4R1-S7, 18.4R2-S4, 18.4R3;
- 19.1 versiones anteriores a 19.1R1-S5, 19.1R2;
- 19.2 versiones anteriores a 19.2R1-S2, 19.2R2;
- 19.3 versiones anteriores a 19.3R2.

Mitigación

- Las siguientes versiones de software se han actualizado para resolver este problema específico: 18.1R3-S9, 18.2R2-S7, 18.2R3-S3, 18.3R1-S7, 18.3R2-S4, 18.3R3-S1, 18.4R1-S7, 18.4R2 -S4, 18.4R3, 19.1R1-S5, 19.1R2, 19.2R1-S2, 19.2R2, 19.3R2, 19.4R1 y todas las versiones posteriores.

Enlaces:

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11031&cat=SIRT_1&actp=LIST

CVE-2020-1641

Problema

Una vulnerabilidad de condición de carrera en la implementación de Juniper Networks Junos OS LLDP permite a un atacante hacer que LLDP se bloquee y provoque una denegación de servicio (DoS). Este problema ocurre cuando el dispositivo recibe paquetes LLDP diseñados desde un dispositivo adyacente. Se producirán múltiples aletas LACP después de que LLDP se bloquee. Un indicador de compromiso es evaluar los detalles del archivo de registro para lldp con RLIMIT. La intervención debe ocurrir antes de que se alcance el umbral del 85% de KB utilizado versus la memoria máxima disponible de KB.

Productos afectados

Este problema afecta a Junos OS 12.3, 12.3X48, 15.1, 15.1X49, 15.1X53, 16.1, 17.1, 17.2, 17.3, 17.4, 18.1, 18.2, 18.2X75, 18.3, 18.4, 19.1.

Juniper Networks Junos OS

- 12.3 versiones anteriores a 12.3R12-S15;
- 12.3X48 versiones anteriores a 12.3X48-D95;
- 15.1 versiones anteriores a 15.1R7-S6;
- 15.1X49 versiones anteriores a 15.1X49-D200;
- 15.1X53 versiones anteriores a 15.1X53-D593;
- 16.1 versiones anteriores a 16.1R7-S7;
- 17.1 versiones anteriores a 17.1R2-S11, 17.1R3-S2;
- 17.2 versiones anteriores a 17.2R1-S9, 17.2R3-S3;
- 17.3 versiones anteriores a 17.3R2-S5, 17.3R3-S6;
- 17.4 versiones anteriores a 17.4R2-S4, 17.4R3;
- 18.1 versiones anteriores a 18.1R3-S5;
- 18.2 versiones anteriores a 18.2R2-S7, 18.2R3;
- Versiones 18.2X75 anteriores a 18.2X75-D12, 18.2X75-D33, 18.2X75-D50, 18.2X75-D420;
- 18.3 versiones anteriores a 18.3R1-S7, 18.3R2-S3, 18.3R3;
- 18.4 versiones anteriores a 18.4R1-S5, 18.4R2;
- 19.1 versiones anteriores a 19.1R1-S4, 19.1R2.

Mitigación

Las siguientes versiones de software se han actualizado para resolver este problema específico: 12.3R12-S15, 12.3X48-D95, 15.1R7-S6, 15.1X49-D200, 15.1X53-D593, 16.1R7-S7, 16.1R7-S7, 17.1R2 - S11, 17.1R3-S2, 17.2R1-S9, 17.2R3-S3, 17.3R2-S5, 17.3R3-S6, 17.4R2-S4, 17.4R3, 18.1R3-S5, 18.2R2-S7, 18.2R3, 18.2 X75-D33, 18.2X75-D50, 18.2X75-D420, 18.3R1-S7, 18.3R2-S3, 18.3R3, 18.4R1-S5, 18.4R2, 19.1R1-S4, 19.1R2, 19.2R1 y todas las versiones posteriores.

Enlaces:

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11027&cat=SIRT_1&actp=LIST

CVE-2020-1645

Problema

Cuando el filtrado de DNS está habilitado en Juniper Networks Junos MX Series con una de las siguientes tarjetas MS-PIC, MS-MIC o MS-MPC, un flujo entrante de paquetes procesados por el proceso de Multiservices PIC Management Daemon (mospmand), responsable de administrar " Servicio de filtrado de URL ", puede bloquearse y provocar que se reinicie el PIC de servicios. Mientras se reinicia el PIC de servicios, todos los servicios de PIC, incluido el servicio de filtrado de DNS (hollow de sumidero de DNS) se omitirán hasta que el PIC de servicios complete su proceso de arranque.

Productos afectados

Este problema afecta a Junos OS 17.3, 18.3, 18.4, 19.1, 19.2, 19.3, 19.4. Plataformas afectadas: Serie MX.

Juniper Networks Junos OS

- 17.3 versiones anteriores a 17.3R3-S8
- 18.3 versiones anteriores a 18.3R2-S4, 18.3R3-S1
- 18.4 versiones anteriores a 18.4R2-S5, 18.4R3
- 19.1 versiones anteriores a 19.1R2-S2, 19.1R3
- 19.2 versiones anteriores a 19.2R1-S5, 19.2R2
- 19.3 versiones anteriores a 19.3R2-S3, 19.3R3
- 19.4 versiones anteriores a 19.4R1-S3, 19.4R2

Mitigación

Las siguientes versiones de software se han actualizado para resolver este problema específico: 18.3R2-S4, 18.3R3-S1, 18.4R2-S5, 18.4R3, 19.1R2-S2, 19.1R3, 19.2R1-S5, 19.2R2, 19.3R2-S3, 19.3R3, 19.4R1-S3, 19.4R2, 20.1R1 y todas las versiones posteriores.

Enlaces:

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11028&cat=SIRT_1&actp=LIST

CVE-2020-1640

Problema

El uso incorrecto de un marco de validación al procesar paquetes BGP genuinos entrantes dentro del demonio RPD de Juniper Networks (proceso de protocolos de enrutamiento) permite que un atacante bloquee el RPD, causando una condición de denegación de servicio (DoS). Este marco requiere que se pasen estos paquetes. Al enviar continuamente cualquiera de estos tipos de paquetes genuinos formateados, un atacante puede bloquear repetidamente el proceso de RPD causando una Denegación de Servicio sostenida. Este problema puede iniciarse o propagarse a través de eBGP e iBGP y puede afectar a los dispositivos en cualquiera de los modos de uso, siempre que los dispositivos estén configurados para admitir el marco comprometido y una ruta BGP esté activada o activa..

Productos afectados

Afecta a Junos OS 17.3, 18.3, 18.4, 19.1, 19.2, 19.3, 19.4. Plataformas afectadas: Serie MX.

Juniper Networks Junos OS

- 16.1 versiones 16.1R7-S6 y versiones posteriores anteriores a 16.1R7-S8
- 17.3 versiones 17.3R2-S5, 17.3R3-S6 y versiones posteriores a 17.3R3-S8
- 17.4 versiones 17.4R2-S7, 17.4R3 y versiones posteriores a 17.4R2-S11, 17.4R3-S2
- 18.1 versiones 18.1R3-S7 y versiones posteriores a 18.1R3-S10
- 18.2 versiones 18.2R2-S6, 18.2R3-S2 y versiones posteriores a 18.2R2-S7, 18.2R3-S5
- 18.2X75 versiones 18.2X75-D12, 18.2X75-D32, 18.2X75-D33, 18.2X75-D51, 18.2X75-D60, 18.2X75-D411, 18.2X75-D420 y versiones posteriores anteriores a 18.2X75-D32, 18.2X75-D33, 18.2X75-D420, 18.2X75-D52, 18.2X75-D60, 18.2X75-D65, 18.2X75-D70
- 18.3 versiones 18.3R1-S6, 18.3R2-S3, 18.3R3 y versiones posteriores a 18.3R2-S4, 18.3R3-S2
- 18.4 versiones 18.4R1-S5, 18.4R2-S4, 18.4R3 y versiones posteriores a 18.4R1-S7, 18.4R2-S5, 18.4R3-S3
- 19.1 versiones 19.1R1-S3, 19.1R2 y versiones posteriores anteriores a 19.1R1-S5, 19.1R2-S2, 19.1R3-S2
- 19.2 versiones 19.2R1-S2, 19.2R2 y versiones posteriores anteriores a 19.2R1-S5, 19.2R2, 19.2R3
- 19.3 versiones anteriores a 19.3R2-S3, 19.3R3
- 19.4 versiones anteriores a 19.4R1-S2, 19.4R2, 19.4R3
- 20.1 versiones anteriores a 20.1R1-S1, 20.1R2

Mitigación

Las siguientes versiones de software se han actualizado para resolver este problema específico: 16.1R7-S8, 17.3R3-S8, 17.4R2-S11, 17.4R3-S2, 18.1R3-S10, 18.2R2-S7, 18.2R3-S5, 18.2X75-D32, 18.2X75-D33, 18.2X75-D420, 18.2X75-D52, 18.2X75-D60, 18.2X75-D65, 18.2X75-D70, 18.3R2-S4, 18.3R3-S2, 18.4R1-S7, 18.4R2-S5, 18.4R3-S3, 19.1R1-S5, 19.1R2-S2, 19.1R3-S2, 19.2R1-S5, 19.2R2, 19.2R3, 19.3R2-S3, 19.3R3, 19.4R1-S2, 19.4R2, 19.4R3, 20.1R1-S1, 20.1R2, 20.2R1 y versiones posteriores.

Enlaces:

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11024&cat=SIRT_1&actp=LIST

CVE-2020-1643

Problema

La ejecución de los comandos " show ospf interface extensive" o " show ospf interface detail" CLI en un dispositivo de Juniper Networks que ejecuta Junos OS puede hacer que el proceso de protocolos de enrutamiento (RPD) se bloquee y reinicie si se configura la autenticación de la interfaz OSPF, lo que lleva a una Denegación de servicio (DoS). Al ejecutar continuamente los mismos comandos de la CLI, un atacante local puede bloquear repetidamente el proceso RPD causando una Denegación de servicio sostenida.

Productos afectados

Este problema afecta a Junos OS 12.3X48, 14.1X53, 15.1, 15.1X49, 15.1X53, 16.1, 17.1, 17.2, 17.3, 17.4, 18.1, 18.2, 18.2X75, 18.3

Juniper Networks Junos OS

- 12.3X48 versiones anteriores a 12.3X48-D100;
- 14.1X53 versiones anteriores a 14.1X53-D140, 14.1X53-D54;
- 15.1 versiones anteriores a 15.1R7-S7;
- 15.1X49 versiones anteriores a 15.1X49-D210;
- 15.1X53 versiones anteriores a 15.1X53-D593;
- 16.1 versiones anteriores a 16.1R7-S8;
- 17.1 versiones anteriores a 17.1R2-S12;
- 17.2 versiones anteriores a 17.2R3-S4;
- 17.3 versiones anteriores a 17.3R3-S8;
- 17.4 versiones anteriores a 17.4R2-S2, 17.4R3;
- 18.1 versiones anteriores a 18.1R3-S2;
- 18.2 versiones anteriores a 18.2R2, 18.2R3;
- Versiones 18.2X75 anteriores a 18.2X75-D40;
- 18.3 versiones anteriores a 18.3R1-S2, 18.3R2.

Mitigación

Las siguientes versiones de software se han actualizado para resolver este problema específico: Junos OS 12.3X48-D100, 14.1X53-D140, 14.1X53-D54, 15.1R7-S7, 15.1X49-D210, 15.1X53-D593, 16.1R7-S8, 17.1R2-S12, 17.2R3-S4, 17.3R3-S8, 17.4R2-S2, 17.4R3, 18.1R3-S2, 18.2R2, 18.2X75-D40, 18.3R1-S2, 18.3R2, 18.4R1 y todos los posteriores lanzamientos.

Enlaces:

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11030&cat=SIRT_1&actp=LIST