Alerta de seguridad informática	9VSA20-00199-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de abril de 2020
Última revisión	30 de abril 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 afecta a actualizaciones.

RESUMEN

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Juniper referente a vulnerabilidad que afecta al Sistema Operativo Junos. El presente informe incluye la respectiva medida de mitigación.

VULNERABILIDAD

CVE-2020-1631

CVE-2020-1631

Impacto

Debido a un error de validación de datos ingresados al procesar secuencias de directorio trasversal en los servicios HTTP/HTTPS utilizados por J-Web, Web Authentication, Firewall Authentication Pass-Through with Web-Redirect y Zero Touch Provisioning (ZTP), un atacante remoto no autenticado podría enviar peticiones HTTP especialmente diseñadas al sistema afectado y lograr la lectura de archivos arbitrarios. Además un atacante podría inyectar comandos en "httpd.log", obteniendo la lectura de ciertos archivos o tokens de sesión de J-Web.

Productos Afectados

Junos OS versiones 12.3, 12.3X48, 14.1X53, 15.1, 15.1X49, 17.2, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4, 19.1, 19.2, 19.3, 19.4 y 20.1.

Mitigación

Juniper ha disponibilizado los siguientes parches para mitigar la vulnerabilidad: 12.3X48-D101, 15.1X49-D211, 18.2R3-S4, 18.4R3-S2 y 20.1R1-S1.
Los parches faltantes serán publicados en el futuro.

Enlaces

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11021&cat=SIRT_1&actp=LIST
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1631