Alerta de seguridad cibernética	9VSA24-00954-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	16 de enero de 2024
Última revisión	16 de enero de 2024

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 CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El CSIRT de Gobierno comparte información de vulnerabilidades parchadas por Juniper en sus firewalls y switches.

Vulnerabilidades

CVE-2016-2183
CVE-2019-17571
CVE-2020-9493
CVE-2021-44228
CVE-2021-44832
CVE-2022-22164
CVE-2022-23302
CVE-2022-23305
CVE-2022-23307
CVE-2023-26464
CVE-2023-36842
CVE-2024-21585
CVE-2024-21587
CVE-2024-21589
CVE-2024-21591
CVE-2024-21594
CVE-2024-21595
CVE-2024-21597
CVE-2024-21599
CVE-2024-21600
CVE-2024-21601
CVE-2024-21602
CVE-2024-21603
CVE-2024-21604
CVE-2024-21606
CVE-2024-21607
CVE-2024-21611
CVE-2024-21612
CVE-2024-21613
CVE-2024-21614
CVE-2022-21699
CVE-2020-0465
CVE-2020-0466
CVE-2021-0920
CVE-2021-26691
CVE-2021-34798
CVE-2021-3564
CVE-2021-3573
CVE-2021-3621
CVE-2021-3752
CVE-2021-39275
CVE-2021-4155
CVE-2021-44790
CVE-2022-0330
CVE-2022-22942
CVE-2024-21617

Impacto

Vulnerabilidades de riesgo crítico:

CVE-2021-44228: Vulnerabilidad en Security Director Insights. CVSS: 10.0. Afecta a las versiones de Juniper Networks Security Director Insights anteriores a la 23.1R1.

CVE-2024-21591: Vulnerabilidad en J-web permite a un actor malicioso basado en la red, causar una denegación de servicio (DoS) o una ejecución remota de código sin autorización, y obtener privilegios de root. CVSS: 9.8. Afecta a todas las versiones de Junos OS en las series SRX y EX.

CVE-2020-9493: Vulnerabilidad en versiones de Apache Chainsaw anteriores a la 2.1.0., que podría llevar a la ejecución remota de código. Afecta a CTPView, versiones anteriores a la 9.1R5.

CVE-2019-17571: Vulnerabilidad que afecta las versiones de Apache Log4j 1.2 hasta la 1.2.17. Afecta a CTPView, versiones anteriores a la 9.1R5.

CVE-2022-23305: Vulnerabilidad en JDBCAppender de Apache Log4j 1.2.x que permite manipular el SQL al ingresar strings diseñados y ejecutar queries SQL no deseados. CVSS: 9.8. Afecta a CTPView, versiones anteriores a la 9.1R5.

CVE-2021-26691: Vulnerabilidad que afecta a Apache HTTP Server 2.4.0. a 2.4.46 que permite provocar un heap overflow enviando una SessionHeader especialmente diseñada. CVSS: 9.8. Afecta a CTPView, versiones anteriores a la 9.1R5.

CVE-2021-44790: Vulnerabilidad que afecta a Apache HTTP Server 2.4.51 y anteriores. Podría provocar buffer overflow. Aplica para routers Juniper Networks Session Smart Router anteriores al SSR-6.2.3-r2.

CVE-2021-39275: Vulnerabilidad en Apache HTTP Server 2.4.48 y anteriores. Aplica para routers Juniper Networks Session Smart Router anteriores al SSR-6.2.3-r2.

CVE-2021-26691: Vulnerabilidad en Apache HTTP Server 2.4.0 a 2.4.46. Aplica para routers Juniper Networks Session Smart Router anteriores al SSR-6.2.3-r2.

Productos afectados

Juniper Networks Junos OS SRX Series y EX Series:
Junos OS versiones anteriores a la 20.4R3-S9;
Junos OS 21.2 versiones anteriores a la 21.2R3-S7;
Junos OS 21.3 versiones anteriores a la 21.3R3-S5;
Junos OS 21.4 versiones anteriores a la 21.4R3-S5;
Junos OS 22.1 versiones anteriores a la 22.1R3-S4;
Junos OS 22.2 versiones anteriores a la 22.2R3-S3;
Junos OS 22.3 versiones anteriores a la 22.3R3-S2;
Junos OS 22.4 versiones anteriores a la 22.4R2-S2, 22.4R3.

Juniper Networks Security Director Insights anteriores a la 23.1R1.

Juniper Networks CTPView, versiones anteriores a la 9.1R5.

Routers Juniper Networks Session Smart Router anteriores al SSR-6.2.3-r2.

Enlaces
https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Security-Director-Insights-Multiple-vulnerabilities-in-SDI?language=en_US
https://supportportal.juniper.net/s/global-search/%40uri?language=en_US#sort=%40sfcec_community_publish_date_formula__c%20descending&numberOfResults=50&f:ctype=[Security%20Advisories]
https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Session-Smart-Router-Multiple-vulnerabilities-resolved?language=en_US

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.01.16 17:51:17 -03'00'