Alerta de seguridad cibernética	9VSA23-00773-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de enero de 2023
Última revisión	16 de enero de 2023

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 sobre vulnerabilidades que afectan a varios productos de Juniper Networks.

Vulnerabilidades

CVE-2019-17571	CVE-2023-22399	CVE-2022-23852	CVE-2021-37576
CVE-2020-8492	CVE-2019-11287	CVE-2022-25235	CVE-2020-0466
CVE-2020-14343	CVE-2023-22398	CVE-2022-25236	CVE-2022-0330
CVE-2020-12049	CVE-2022-0778	CVE-2022-25315	CVE-2020-12362
CVE-2020-14583	CVE-2023-22416	CVE-2021-3177	CVE-2021-22555
CVE-2020-14593	CVE-2023-22401	CVE-2021-39275	CVE-2021-29154
CVE-2020-27223	CVE-2023-22415	CVE-2021-44790	CVE-2021-33033
CVE-2021-21309	CVE-2023-22412	CVE-2022-22720	CVE-2021-33034
CVE-2022-22184	CVE-2023-22394	CVE-2022-2526	CVE-2021-3347
CVE-2007-6755	CVE-2023-22393	CVE-2021-26691	CVE-2021-33909
CVE-2019-1543	CVE-2023-22391	CVE-2016-4658	CVE-2021-3715
CVE-2019-1551	CVE-2023-22414	CVE-2021-40438	CVE-2021-4034
CVE-2023-22397	CVE-2023-22411	CVE-2022-22825	CVE-2021-4028
CVE-2020-28469	CVE-2023-22396	CVE-2022-22826	CVE-2021-27365
CVE-2021-23840	CVE-2023-22405	CVE-2022-22827	CVE-2022-0492
CVE-2021-3712	CVE-2023-22400	CVE-2021-3621	CVE-2021-22543
CVE-2021-3765	CVE-2023-22410	CVE-2021-45960	CVE-2021-34798
CVE-2023-22403	CVE-2023-22404	CVE-2022-1271	CVE-2020-27827
CVE-2023-22407	CVE-2023-22395	CVE-2020-24489	CVE-2020-35498
CVE-2023-22409	CVE-2023-22417	CVE-2021-30465	CVE-2018-25032
CVE-2021-3156	CVE-2023-22402	CVE-2020-14583	CVE-2021-23840
CVE-2020-14145	CVE-2023-22413	CVE-2021-42574	CVE-2021-27219
CVE-2020-14871	CVE-2022-22822	CVE-2022-24903	CVE-2022-0778
CVE-2023-22408	CVE-2022-22823	CVE-2021-46143	CVE-2022-38177
CVE-2023-22406	CVE-2022-22824	CVE-2020-36385	CVE-2022-38178

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

https://www.csirt.gob.cl
Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl
@csirtgob
https://www.linkedin.com/company/csirt-gob

CVE-2022-21449	CVE-2020-12363	CVE-2022-21341	CVE-2020-14797
CVE-2022-34169	CVE-2020-12364	CVE-2022-21349	CVE-2022-21248
CVE-2022-21476	CVE-2021-29650	CVE-2022-21360	CVE-2020-14577
CVE-2021-2388	CVE-2020-25704	CVE-2022-21365	CVE-2020-14581
CVE-2020-14593	CVE-2020-36322	CVE-2022-21366	CVE-2021-35603
CVE-2022-29154	CVE-2020-0543	CVE-2020-14621	CVE-2020-14781
CVE-2021-3712	CVE-2020-0548	CVE-2022-21434	CVE-2020-24512
CVE-2021-25217	CVE-2020-0549	CVE-2022-21496	CVE-2020-14798
CVE-2020-26116	CVE-2020-8695	CVE-2022-21549	CVE-2021-2341
CVE-2020-8648	CVE-2020-8696	CVE-2021-35564	CVE-2020-14796
CVE-2021-27364	CVE-2020-8698	CVE-2022-21291	CVE-2022-22942
CVE-2021-3752	CVE-2021-4155	CVE-2022-21305	CVE-2022-29154
CVE-2021-32399	CVE-2022-21123	CVE-2022-21540	CVE-2022-2526
CVE-2022-1729	CVE-2022-21125	CVE-2020-14803	CVE-2022-21541
CVE-2021-4083	CVE-2022-21166	CVE-2022-21282	CVE-2022-34169
CVE-2020-0465	CVE-2021-3504	CVE-2022-21296	CVE-2022-21540
CVE-2021-35567	CVE-2020-14562	CVE-2021-2163	CVE-2022-21624
CVE-2021-42739	CVE-2022-21426	CVE-2019-20934	CVE-2022-21626
CVE-2020-26137	CVE-2021-35556	CVE-2020-14556	CVE-2022-21628
CVE-2021-40085	CVE-2021-35559	CVE-2020-27170	CVE-2022-21619
CVE-2020-24511	CVE-2021-35561	CVE-2021-27363	CVE-2007-2285
CVE-2020-24513	CVE-2021-35565	CVE-2021-2369	CVE-2018-8046
CVE-2021-0920	CVE-2021-35578	CVE-2020-14792	CVE-2020-26137
CVE-2021-3573	CVE-2021-35586	CVE-2020-14578	CVE-2021-3177
CVE-2021-23841	CVE-2022-21277	CVE-2020-14579	CVE-2020-26116
CVE-2022-21541	CVE-2022-21283	CVE-2021-2432	CVE-2022-1729
CVE-2021-2161	CVE-2022-21293	CVE-2022-21443	CVE-2022-32250
CVE-2021-35550	CVE-2022-21294	CVE-2020-14779	CVE-2022-1271
CVE-2020-11668	CVE-2022-21299	CVE-2020-14573	
CVE-2021-3564	CVE-2022-21340	CVE-2020-14782	

Impacto

Vulnerabilidades de riesgo crítico

CVE-2019-17571: Incluida en Log4j 1.2 está una clase de SocketServer vulnerable a deserialización de datos no confiables, que puede ser explotado para ejecutar código arbitrario.

CVE-2020-14343: Vulnerabilidad descubierta en las bibliotecas PyYAML anteriores a la versión 5.4, susceptibles a la ejecución arbitraria de código cuando procesan archivos YAML no confiables a través del método full_load o con el loader FullLoader.

CVE-2020-14871: Vulnerabilidad en un software de una tercera parte, incluido en Contrail Service Orchestration (CSO).

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

Contrail Cloud in release 13.7.0.
Contrail Networking anteriores a la versión 2011.
Contrail Networking versiones posteriores a R22.1 y anteriores a R22.3.
Contrail Service Orchestration (CSO) anterior a 6.3.0.
Junos OS 12.3 version 12.3R12-S19 and later versions.
Junos OS 15.1 version 15.1R7-S10 and later versions.
Junos OS 15.1 versions prior to 15.1R7-S12.
Junos OS 17.3 version 17.3R3-S12 and later versions.
Junos OS 18.4 version 18.4R3-S9 and later versions.
Junos OS 19.1 version 19.1R3-S7 and later versions.
Junos OS 19.1 versions prior to 19.1R3-S9.
Junos OS 19.2 version 19.2R3-S3 and later versions.
Junos OS 19.2 versions prior to 19.2R1-S9, 19.2R3-S5.
Junos OS 19.3 version 19.3R2-S7, 19.3R3-S3 and later versions prior to 19.3R3-S7.
Junos OS 19.3 versions prior to 19.3R3-S6.
Junos OS 19.4 version 19.4R2-S7, 19.4R3-S5 and later versions prior to 19.4R3-S10.
Junos OS 19.4 versions prior to 19.4R2-S7, 19.4R3-S8.
Junos OS 19.4 versions prior to 19.4R3-S9.
Junos OS 20.1 version 20.1R1 and later versions.
Junos OS 20.1 version 20.1R3-S1 and later versions.
Junos OS 20.1 versions prior to 20.1R3-S4.
Junos OS 20.2 version 20.2R3-S2 and later versions prior to 20.2R3-S6.
Junos OS 20.2 versions prior to 20.2R3-S5.
Junos OS 20.2 versions prior to 20.2R3-S5.
Junos OS 20.3 version 20.3R3-S1 and later versions prior to 20.3R3-S6.
Junos OS 20.3 versions prior to 20.3R3-S5.
Junos OS 20.3 versions prior to 20.3R3-S5.
Junos OS 20.4 version 20.4R2-S2, 20.4R3 and later versions prior to 20.4R3-S5.
Junos OS 20.4 versions prior to 20.4R3-S4.
Junos OS 20.4 versions prior to 20.4R3-S4.
Junos OS 21.1 version 21.1R2 and later versions prior to 21.1R3-S4.
Junos OS 21.1 versions prior to 21.1R1-S1, 21.1R2.
Junos OS 21.1 versions prior to 21.1R3-S3.
Junos OS 21.2 version 21.2R1-S1, 21.2R2 and later versions prior to 21.2R3-S3.
Junos OS 21.2 versions prior to 21.2R3-S2.
Junos OS 21.3 versions prior to 21.3R3-S1.
Junos OS 21.3 versions prior to 21.3R3-S2.
Junos OS 21.4 versions prior to 21.4R3.
Junos OS 21.4 versions prior to 21.4R3.
Junos OS 22.1 versions prior to 22.1R2.
Junos OS 22.1 versions prior to 22.1R2-S1, 22.1R3.
Junos OS 22.2 versions prior to 22.2R1-S2, 22.2R2.
Junos OS 22.3 versions prior to 22.3R1-S1, 22.3R2.

Junos OS All versions prior to 19.3R3-S7.
Junos OS Evolved 21.1 versions prior to 21.1R2-EVO.
Junos OS Evolved 21.1-EVO version 21.1R1-EVO and later versions.
Junos OS Evolved 21.2-EVO versions prior to 21.2R3-S4-EVO.
Junos OS Evolved 21.3 versions prior to 21.3R3-EVO.
Junos OS Evolved 21.3-EVO version 21.3R1-EVO and later versions.
Junos OS Evolved 21.4 versions prior to 21.4R2-EVO.
Junos OS Evolved 21.4-EVO versions prior to 21.4R2-EVO.
Junos OS Evolved 22.1 versions prior to 22.1R2-EVO.
Junos OS Evolved 22.1-EVO versions prior to 22.1R3-EVO.
Junos OS Evolved 22.2 versions prior to 22.2R1-S1-EVO, 22.2R2-EVO.
Junos OS Evolved All versions prior to 20.4R3-S3-EVO.
Junos OS Evolved All versions prior to 20.4R3-S4.
Junos OS Evolved on PTX10003 21.3 versions prior to 21.3R3-S1-EVO.
Junos OS Evolved on PTX10003 All versions prior to 20.4R3-S4-EVO.
Junos OS Evolved on PTX1000321.4 versions prior to 21.4R2-S2-EVO, 21.4R3-EVO.
Junos OS Evolved on PTX1000322.1 versions prior to 22.1R1-S2-EVO, 22.1R2-EVO.
Junos OS Evolved on PTX1000322.2 versions prior to 22.2R2-EVO.
Junos OS Evolved versión 22.3R1-EVO.
Junos OS Evolved19.3 versions prior to 19.3R3-EVO.
Junos OS Evolved19.4 versions prior to 19.4R3-EVO.
Junos OS Evolved20.1 versions prior to 20.1R3-EVO.
Junos OS Evolved20.2 versions prior to 20.2R2-EVO.
Junos OS Evolved21.1 versions prior to 21.1R2-EVO.
Junos OS Evolved21.2 version 21.2R1 and later versions.
Junos OS Evolved21.3 versions prior to 21.3R2-EVO.
Junos OS Evolved21.3-EVO version 21.3R3-EVO and later versions.
Junos OS Evolved21.4 versions prior to 21.4R2-S1-EVO, 21.4R3-EVO.
Junos OS Evolved21.4-EVO version 21.4R1-S2-EVO, 21.4R2-EVO and later prior to 21.4R2-S1-EVO.
Junos OS Evolved21.4-EVO versions prior to 21.4R2-S2-EVO, 21.4R3-EVO.
Junos OS Evolved22.1 versions prior to 22.1R2-EVO.
Junos OS Evolved22.1-EVO version 22.1R2-EVO and later versions prior to 22.1R3-EVO.
Junos OS Evolved22.1-EVO versions prior to 22.1R1-S2-EVO, 22.1R2-EVO.
Junos OS Evolved22.2-EVO versions prior to 22.2R1-S1-EVO, 22.2R2-EVO.
Junos OS Evolved22.2-EVO versions prior to 22.2R1-S1-EVO, 22.2R2-EVO.
Junos OS EvolvedAll versions prior to 19.2R3-EVO.
Junos OS EvolvedAll versions prior to 20.4R2-EVO.
Junos OS EvolvedAll versions prior to 20.4R3-S4-EVO.
Junos OS on ACX2K Series 20.3 versions prior to 20.3R3-S6.
Junos OS on ACX2K Series 20.4 versions prior to 20.4R3-S4.
Junos OS on ACX2K Series 21.2 versions prior to 21.2R3-S3.
Junos OS on ACX2K Series All 20.2 versions.
Junos OS on ACX2K Series All 21.1 versions.
Junos OS on ACX2K Series All versions prior to 19.4R3-S9.
Junos OS on MX Series 20.3 version 20.3R1 and later versions.
Junos OS on MX Series All versions prior to 20.2R3-S5.

Junos OS on MX Series and SRX Series20.2 versions prior to 20.2R3-S6.
Junos OS on MX Series and SRX Series20.3 versions prior to 20.3R3-S6.
Junos OS on MX Series and SRX Series20.4 versions prior to 20.4R3-S5.
Junos OS on MX Series and SRX Series20.4 versions prior to 20.4R3-S5.
Junos OS on MX Series and SRX Series21.1 versions prior to 21.1R3-S4.
Junos OS on MX Series and SRX Series21.1 versions prior to 21.1R3-S4.
Junos OS on MX Series and SRX Series21.2 versions prior to 21.2R3-S2.
Junos OS on MX Series and SRX Series21.2 versions prior to 21.2R3-S3.
Junos OS on MX Series and SRX Series21.3 versions prior to 21.3R3-S1.
Junos OS on MX Series and SRX Series21.3 versions prior to 21.3R3-S3.
Junos OS on MX Series and SRX Series21.4 versions prior to 21.4R3.
Junos OS on MX Series and SRX Series21.4 versions prior to 21.4R3.
Junos OS on MX Series and SRX Series22.1 versions prior to 22.1R1-S2, 22.1R2.
Junos OS on MX Series and SRX Series22.1 versions prior to 22.1R2-S1, 22.1R3.
Junos OS on MX Series and SRX Series22.2 versions prior to 22.2R1-S1, 22.2R2.
Junos OS on MX Series and SRX Series22.2 versions prior to 22.2R1-S2, 22.2R2.
Junos OS on MX Series and SRX SeriesAll versions prior to 19.4R3-S10.
Junos OS on MX Series20.1 version 20.1R3-S5 and later versions.
Junos OS on MX Series20.2 versions prior to 20.2R3-S5.
Junos OS on MX Series20.3 versions prior to 20.3R3-S5.
Junos OS on MX Series20.4 versions prior to 20.4R3-S4.
Junos OS on MX Series21.1 versions prior to 21.1R3-S3.
Junos OS on MX Series21.2 versions prior to 21.2R3-S1.
Junos OS on MX Series21.3 versions prior to 21.3R3.
Junos OS on MX Series21.4 versions prior to 21.4R2-S1, 21.4R3.
Junos OS on MX Series22.1 versions prior to 22.1R2.
Junos OS on MX SeriesAll versions prior to 19.4R3-S9.
Junos OS on QFX10K Series 20.2 versions prior to 20.2R3-S6.
Junos OS on QFX10K Series 20.3 versions prior to 20.3R3-S6.
Junos OS on QFX10K Series 20.4 versions prior to 20.4R3-S5.
Junos OS on QFX10K Series 21.1 versions prior to 21.1R3-S4.
Junos OS on QFX10K Series 21.2 versions prior to 21.2R3-S3.
Junos OS on QFX10K Series 21.3 versions prior to 21.3R3-S2.
Junos OS on QFX10K Series 21.4 versions prior to 21.4R2-S2, 21.4R3.
Junos OS on QFX10K Series 22.1 versions prior to 22.1R2.
Junos OS on QFX10K Series 22.2 versions prior to 22.2R1-S2, 22.2R2.
Junos OS on QFX10K Series All versions prior to 19.4R3-S9.
Junos OS on QFX10K Series:
Junos OS on QFX5k Series, EX46xx Series
Junos OS on QFX5k Series, EX46xx Series 20.3 versions prior to 20.3R3-S5.
Junos OS on QFX5k Series, EX46xx Series 20.4 versions prior to 20.4R3-S4.
Junos OS on QFX5k Series, EX46xx Series 21.1 versions prior to 21.1R3-S3.
Junos OS on QFX5k Series, EX46xx Series 21.2 versions prior to 21.2R3-S1.
Junos OS on QFX5k Series, EX46xx Series 21.3 versions prior to 21.3R3 on.
Junos OS on QFX5k Series, EX46xx Series 21.4 versions prior to 21.4R3 on.
Junos OS on QFX5k Series, EX46xx Series 22.1 versions prior to 22.1R2 on.

Junos OS on QFX5k Series, EX46xx Series All versions prior to 20.2R3-S5.
Junos OS on SRX 5000 Series 20.4 versions prior to 20.4R3-S5.
Junos OS on SRX 5000 Series 21.1 versions prior to 21.1R3-S4.
Junos OS on SRX 5000 Series 21.2 versions prior to 21.2R3-S3.
Junos OS on SRX 5000 Series 21.3 versions prior to 21.3R3-S3.
Junos OS on SRX 5000 Series 21.4 versions prior to 21.4R3-S2.
Junos OS on SRX 5000 Series 22.1 versions prior to 22.1R2-S2, 22.1R3.
Junos OS on SRX 5000 Series 22.2 versions prior to 22.2R3.
Junos OS on SRX 5000 Series 22.3 versions prior to 22.3R1-S1, 22.3R2.
Junos OS on SRX Series 19.2 versions prior to 19.2R3-S6.
Junos OS on SRX Series 19.3 versions prior to 19.3R3-S6.
Junos OS on SRX Series 19.4 versions prior to 19.4R2-S8, 19.4R3-S10.
Junos OS on SRX Series 19.4 versions prior to 19.4R3-S9.
Junos OS on SRX Series 20.2 versions prior to 20.2R3-S5.
Junos OS on SRX Series 20.2 versions prior to 20.2R3-S6.
Junos OS on SRX Series 20.3 versions prior to 20.3R3-S4.
Junos OS on SRX Series 20.3 versions prior to 20.3R3-S5.
Junos OS on SRX Series 20.4 versions prior to 20.4R3-S3.
Junos OS on SRX Series 20.4 versions prior to 20.4R3-S5.
Junos OS on SRX Series 21.1 versions prior to 21.1R3.
Junos OS on SRX Series 21.1 versions prior to 21.1R3-S4.
Junos OS on SRX Series 21.2 versions prior to 21.2R3.
Junos OS on SRX Series 21.2 versions prior to 21.2R3.
Junos OS on SRX Series 21.3 versions prior to 21.3R2.
Junos OS on SRX Series 21.3 versions prior to 21.3R3.
Junos OS on SRX Series 21.4 versions prior to 21.4R2.
Junos OS on SRX Series 21.4 versions prior to 21.4R2.
Junos OS on SRX Series All versions prior to 19.3R3-S7.
Junos OS on SRX Series and on MX Series 19.4 versions prior to 19.4R2-S8, 19.4R3-S10.
Junos OS on SRX Series and on MX Series 20.1 versions 20.1R1 and later versions.
Junos OS on SRX Series and on MX Series 20.2 versions prior to 20.2R3-S6.
Junos OS on SRX Series and on MX Series 20.3 versions prior to 20.3R3-S6.
Junos OS on SRX Series and on MX Series 20.4 versions prior to 20.4R3-S5.
Junos OS on SRX Series and on MX Series 21.1 versions prior to 21.1R3-S5.
Junos OS on SRX Series and on MX Series 21.2 versions prior to 21.2R3-S1.
Junos OS on SRX Series and on MX Series 21.3 versions prior to 21.3R3.
Junos OS on SRX Series and on MX Series 21.4 versions prior to 21.4R2-S2, 21.4R3.
Junos OS on SRX Series and on MX Series 22.1 versions prior to 22.1R1-S2, 22.1R2, 22.1R3-S1.
Junos OS on SRX Series and on MX Series All versions prior to 19.3R3-S7.
Junos OS on SRX Series, and MX Series with SPC3 19.4 versions prior to 19.4R3-S9.
Junos OS on SRX Series, and MX Series with SPC3 20.1 version 20.1R1 and later versions.
Junos OS on SRX Series, and MX Series with SPC3 All versions prior to 19.3R3-S7.
Junos OS on SRX Series, and MX Series with SPC3 All versions prior to 19.4R3-S10.
Junos OS on SRX Series, and MX Series with SPC320.2 versions prior to 20.2R3-S5.
Junos OS on SRX Series, and MX Series with SPC320.2 versions prior to 20.2R3-S6.
Junos OS on SRX Series, and MX Series with SPC320.3 versions prior to 20.3R3-S5.

Junos OS on SRX Series, and MX Series with SPC320.3 versions prior to 20.3R3-S6.
Junos OS on SRX Series, and MX Series with SPC320.4 versions prior to 20.4R3-S4.
Junos OS on SRX Series, and MX Series with SPC320.4 versions prior to 20.4R3-S5.
Junos OS on SRX Series, and MX Series with SPC321.1 versions prior to 21.1R3-S3.
Junos OS on SRX Series, and MX Series with SPC321.1 versions prior to 21.1R3-S4.
Junos OS on SRX Series, and MX Series with SPC321.2 versions prior to 21.2R3-S2.
Junos OS on SRX Series, and MX Series with SPC321.2 versions prior to 21.2R3-S3.
Junos OS on SRX Series, and MX Series with SPC321.3 versions prior to 21.3R3-S1.
Junos OS on SRX Series, and MX Series with SPC321.3 versions prior to 21.3R3-S3.
Junos OS on SRX Series, and MX Series with SPC321.4 versions prior to 21.4R2-S1, 21.4R3.
Junos OS on SRX Series, and MX Series with SPC321.4 versions prior to 21.4R3-S1.
Junos OS on SRX Series, and MX Series with SPC322.1 versions prior to 22.1R1-S2, 22.1R2.
Junos OS on SRX Series, and MX Series with SPC322.1 versions prior to 22.1R2-S2, 22.1R3.
Junos OS on SRX Series, and MX Series with SPC322.2 versions prior to 22.2R2.
Junos OS PTX Series and QFX10000 Series20.2 versions prior to 20.2R3-S6.
Junos OS PTX Series and QFX10000 Series20.3 versions prior to 20.3R3-S6.
Junos OS PTX Series and QFX10000 Series20.4 versions prior to 20.4R3-S4.
Junos OS PTX Series and QFX10000 Series21.1 versions prior to 21.1R3-S3.
Junos OS PTX Series and QFX10000 Series21.2 versions prior to 21.2R3-S1.
Junos OS PTX Series and QFX10000 Series21.3 versions prior to 21.3R3.
Junos OS PTX Series and QFX10000 Series21.4 versions prior to 21.4R3.
Junos OS PTX Series and QFX10000 Series22.1 versions prior to 22.1R2.
Junos OS PTX Series and QFX10000 Series22.2 versions prior to 22.2R2.
Junos OS versión 22.3R1.
Junos OS:20.4 versions prior to 20.4R3-S4.
Junos OS:21.1 versions prior to 21.1R3-S3.
Junos OS:21.2 versions prior to 21.2R3-S1.
Junos OS:21.3 versions prior to 21.3R3.
Junos OS:21.4 versions prior to 21.4R3.
Junos OS:22.1 versions prior to 22.1R2.
Junos OS All versions prior to 20.2R3-S7.
Junos OS19.1 versions prior to 19.1R3-S2.
Junos OS19.2 version 19.2R1 and later versions.
Junos OS19.2 versions prior to 19.2R3.
Junos OS19.3 versions prior to 19.3R3.
Junos OS19.3 versions prior to 19.3R3-S6.
Junos OS19.4 versions prior to 19.4R2-S7, 19.4R3-S9.
Junos OS19.4 versions prior to 19.4R2-S8, 19.4R3-S9.
Junos OS19.4 versions prior to 19.4R3.
Junos OS20.1 versions prior to 20.1R2.
Junos OS20.1 versions prior to 20.1R3-S4.
Junos OS20.2 versions prior to 20.2R2.
Junos OS20.2 versions prior to 20.2R3-S5.
Junos OS20.2 versions prior to 20.2R3-S5.
Junos OS20.3 versions prior to 20.3R3-S4.
Junos OS20.3 versions prior to 20.3R3-S5.

Junos OS20.4 versions prior to 20.4R3-S4.
Junos OS20.4 versions prior to 20.4R3-S4.
Junos OS21.1 versions prior to 21.1R3-S3.
Junos OS21.1 versions prior to 21.1R3-S3.
Junos OS21.1 versions prior to 21.1R3-S4.
Junos OS21.2 versions prior to 21.2R3-S1.
Junos OS21.2 versions prior to 21.2R3-S2.
Junos OS21.2 versions prior to 21.2R3-S3.
Junos OS21.3 versions prior to 21.3R3-S1.
Junos OS21.3 versions prior to 21.3R3-S1.
Junos OS21.3 versions prior to 21.3R3-S2.
Junos OS21.4 versions prior to 21.4R2.
Junos OS21.4 versions prior to 21.4R2-S1, 21.4R3.
Junos OS21.4 versions prior to 21.4R2-S2, 21.4R3.
Junos OS22.1 version 22.1R2 and later versions.
Junos OS22.1 versions prior to 22.1R1-S2, 22.1R2.
Junos OS22.1 versions prior to 22.1R2.
Junos OS22.1 versions prior to 22.1R2.
Junos OS22.1 versions prior to 22.1R3.
Junos OS22.2 versions prior to 22.2R1-S1, 22.2R2.
Junos OS22.2 versions prior to 22.2R2.
Junos OSAll versions prior to 18.4R2-S7.
Junos OSAll versions prior to 19.1R3-S9.
Junos OSAll versions prior to 19.3R3-S7.
Junos Space versions prior to 22.3R1.
NorthStar Controller versions prior to 6.2.3.

Enlaces

https://supportportal.juniper.net/s/article/2022-01-Security-Bulletin-Contrail-Networking-Multiple-Vulnerabilities-have-been-resolved-in-Contrail-Networking-release-2011?language=en_US
https://supportportal.juniper.net/s/article/2022-12-Out-of-Cycle-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-A-BGP-session-will-flap-upon-receipt-of-a-specific-optional-transitive-attribute-in-version-22-3R1-CVE-2022-22184?language=en_US
https://supportportal.juniper.net/s/article/2022-10-Security-Bulletin-Contrail-Networking-Multiple-Vulnerabilities-have-been-resolved-in-Contrail-Networking-R22-3?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-QFX10k-Series-ICCP-flap-will-be-observed-due-to-excessive-specific-traffic-CVE-2023-22403?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-Evolved-PTX10003-An-attacker-sending-specific-genuine-packets-will-cause-a-memory-leak-in-the-PFE-leading-to-a-Denial-of-Service-CVE-2023-22397?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-An-RPD-crash-can-happen-due-to-an-MPLS-TE-tunnel-configuration-change-on-a-directly-connected-router-CVE-2023-22407?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-SRX-Series-MX-Series-with-SPC3-When-an-inconsistent-NAT-configuration-exists-and-a-specific-CLI-command-is-issued-the-SPC-will-reboot-CVE-2023-22409?language=en_US

https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Contrail-Service-Orchestration-Multiple-vulnerabilities-resolved-in-CSO-6-3-0?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-SRX-5000-Series-Upon-processing-of-a-specific-SIP-packet-an-FPC-can-crash-CVE-2023-22408?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-A-memory-leak-which-will-ultimately-lead-to-an-rpd-crash-will-be-observed-when-a-peer-interface-flaps-continuously-in-a-Segment-Routing-scenario-CVE-2023-22406?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Northstar-Controller-Pivotal-RabbitMQ-contains-a-web-management-plugin-that-is-vulnerable-to-a-Denial-of-Service-DoS-attack-CVE-2019-11287?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-QFX10K-Series-PFE-crash-upon-receipt-of-specific-genuine-packets-when-sFlow-is-enabled-CVE-2023-22399?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-RPD-might-crash-when-MPLS-ping-is-performed-on-BGP-LSPs-CVE-2023-22398?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-OpenSSL-Infinite-loop-in-BN-mod-sqrt-reachable-when-parsing-certificates-CVE-2022-0778?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-SRX-Series-The-flowd-daemon-will-crash-if-SIP-ALG-is-enabled-and-a-malicious-SIP-packet-is-received-CVE-2023-22416?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-PTX10008-PTX10016-When-a-specific-SNMP-MIB-is-queried-the-FPC-will-crash-CVE-2023-22401?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-MX-Series-and-SRX-Series-The-flow-processing-daemon-flowd-will-crash-when-a-specific-H-323-packet-is-received-CVE-2023-22415?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-MX-Series-and-SRX-Series-The-flowd-daemon-will-crash-if-the-SIP-ALG-is-enabled-and-specific-SIP-messages-are-processed-CVE-2023-22412?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-SRX-Series-and-MX-Series-Memory-leak-due-to-receipt-of-specially-crafted-SIP-calls-CVE-2023-22394?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-RPD-crash-upon-receipt-of-BGP-route-with-invalid-next-hop-CVE-2023-22393?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-ACX2K-Series-Receipt-of-a-high-rate-of-specific-traffic-will-lead-to-a-Denial-of-Service-DoS-CVE-2023-22391?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-PTX-Series-and-QFX10000-Series-An-FPC-memory-leak-is-observed-when-specific-multicast-packets-are-processed-CVE-2023-22414?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-SRX-Series-The-flowd-daemon-will-crash-when-Unified-Policies-are-used-with-IPv6-and-certain-dynamic-applications-are-rejected-by-the-device-CVE-2023-22411?language=en_US

https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-Space-Multiple-vulnerabilities-resolved-in-22-3R1-release?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-MX-Series-FPC-crash-when-an-IPsec6-tunnel-processes-specific-IPv4-packets-CVE-2023-22413?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-Evolved-The-kernel-might-restart-in-a-BGP-scenario-where-bgp-auto-discovery-is-enabled-and-such-a-neighbor-flaps-CVE-2023-22402?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-SRX-Series-A-memory-leak-might-be-observed-in-IPsec-VPN-scenario-leading-to-an-FPC-crash-CVE-2023-22417?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Contrail-Cloud-Multiple-Vulnerabilities-have-been-resolved-in-Contrail-Cloud-release-13-7-0?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-In-an-MPLS-scenario-the-processing-of-specific-packets-to-the-device-causes-a-buffer-leak-and-ultimately-a-loss-of-connectivity-CVE-2023-22395?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-SRX-Series-and-MX-Series-with-SPC3-When-IPsec-VPN-is-configured-iked-will-core-when-a-specifically-formatted-payload-is-received-CVE-2023-22404?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-Evolved-Multiple-vulnerabilities-resolved-in-OpenSSL?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-MX-Series-with-MPC10-MPC11-When-Suspicious-Control-Flow-Detection-scfd-is-enabled-and-an-attacker-is-sending-specific-traffic-this-causes-a-memory-leak-CVE-2023-22410?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-Evolved-A-specific-SNMP-GET-operation-and-a-specific-CLI-commands-cause-resources-to-leak-and-eventually-the-evo-pfemand-process-will-crash-CVE-2023-22400?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-QFX5k-Series-EX46xx-Series-MAC-limiting-feature-stops-working-after-PFE-restart-device-reboot--CVE-2023-22405?language=en_US
https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Junos-OS-Receipt-of-crafted-TCP-packets-on-Ethernet-console-port-results-in-MBUF-leak-leading-to-Denial-of-Service-DoS-CVE-2023-22396?language=en_US
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17571
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8492
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14343
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12049
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14583
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14593
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27223
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21309
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22184
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6755
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1543
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1551
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22397
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28469

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23840
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3712
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3765
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22403
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22407
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22409
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3156
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14145
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14871
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22408
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22406
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22399
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11287
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22398
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0778
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22416
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22401
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22415
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22412
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22394
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22393
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22391
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22414
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22411
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22396
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22405
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22400
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22410
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22404
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22404
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22417
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22402
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22413
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22822
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22823
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22824
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23852
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25235
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25236
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25315
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3177
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39275
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44790
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22720
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2526
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26691

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4658
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40438
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22825
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22826
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22827
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3621
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45960
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1271
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24489
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30465
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14583
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42574
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24903
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46143
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-36385
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37576
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0466
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0330
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12362
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22555
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29154
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33033
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33034
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3347
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33909
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3715
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4034
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4028
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27365
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0492
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22543
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34798
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27827
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-35498
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-25032
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23840
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27219
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0778
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38177
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38178
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21449
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34169
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21476
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-2388
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14593
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29154

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3712
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25217
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26116
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8648
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27364
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3752
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-32399
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1729
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4083
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0465
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35567
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42739
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26137
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40085
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24511
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24513
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0920
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3573
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23841
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21541
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-2161
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35550
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11668
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3564
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12363
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12364
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29650
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25704
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-36322
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0543
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0548
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0549
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8695
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8696
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8698
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4155
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21123
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21125
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21166
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3504
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14562
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21426
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35556
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35559
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35561
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35565

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35578
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35586
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21277
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21283
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21293
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21294
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21299
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21340
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21341
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21349
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21360
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21365
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21366
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14621
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21434
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21496
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21549
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35564
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21291
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21305
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21540
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14803
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21282
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21296
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-2163
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20934
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14556
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27170
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27363
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-2369
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14792
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14578
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14579
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-2432
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21443
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14779
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14573
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14782
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14797
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21248
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14577
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14581
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35603
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14781
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24512
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14798

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-2341
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14796
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22942
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29154
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2526
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21541
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34169
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21540
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21624
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21626
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21628
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21619
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2285
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8046
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26137
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3177
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26116
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1729
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32250
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1271

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.01.17 10:12:25 -03'00'