

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Coordinación Nacional de Ciberseguridad
Ministerio del Interior y Seguridad Pública
Gobierno de Chile



Alerta de seguridad cibernética	9VSA23-00924-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	24 de octubre de 2023
Última revisión	24 de octubre 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 de las actualizaciones de seguridad recientemente publicadas por Juniper para Junos OS y Junos OS Evolved.

Vulnerabilidades

CVE-2023-44194	CVE-2023-44199
CVE-2023-44190	CVE-2023-44188
CVE-2023-44189	CVE-2023-44191
CVE-2023-36839	CVE-2023-22392
CVE-2023-44204	CVE-2023-44192
CVE-2023-44182	CVE-2023-44175
CVE-2023-44203	CVE-2023-36841
CVE-2023-44202	CVE-2023-36843
CVE-2023-44198	CVE-2023-44193
CVE-2023-44197	CVE-2023-44183
CVE-2023-44196	CVE-2023-44185
CVE-2023-44195	CVE-2023-44176
CVE-2023-44187	CVE-2023-44177
CVE-2023-44201	CVE-2023-44178

Impacto

Vulnerabilidades de alto riesgo

CVE-2022-44194: Vulnerabilidad que entrega permisos incorrectos por default, y que permite a un atacante no autenticado con acceso local a un dispositivo vulnerable crear una puerta trasera con privilegios de root. CVSS: 8.4.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Coordinación Nacional de Ciberseguridad
Ministerio del Interior y Seguridad Pública
Gobierno de Chile



Productos afectados

Junos OS y Junos OS Evolved

Enlaces

[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/global-search/%40uri?language=en_US#sort=%40sfcec_community_publish_date_formula__c%20descending&numberOfResults=50&f:ctype=[Security%20Advisories])
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44194>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44190>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44189>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36839>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44204>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44182>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44203>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44202>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44198>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44197>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44196>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44195>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44187>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44201>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44199>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44188>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44191>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22392>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44192>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44175>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36841>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36843>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44193>