Alerta de seguridad cibernética	9VSA23-00863-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de julio de 2023
Última revisión	13 de julio 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 nuevas vulnerabilidades parchadas por Juniper Networks en Junos OS.

Vulnerabilidades

CVE-2022-31629	CVE-2021-21702	CVE-2022-2588	CVE-2020-13946
CVE-2022-31628	CVE-2020-7071	CVE-2022-26373	CVE-2022-38023
CVE-2022-31627	CVE-2017-7653	CVE-2022-29900	CVE-2022-42703
CVE-2022-31626	CVE-2017-7654	CVE-2022-29901	CVE-2022-4378
CVE-2022-31625	CVE-2017-7655	CVE-2022-30123	CVE-2021-25220
CVE-2021-21708	CVE-2020-13817	CVE-2022-3276	CVE-2022-2795
CVE-2021-21707	CVE-2020-11868	CVE-2022-41974	CVE-2023-36838
CVE-2021-21705	CVE-2019-11358	CVE-2022-42898	CVE-2023-36849
CVE-2021-21704	CVE-2021-40085	CVE-2021-26401	CVE-2023-36835
CVE-2021-21703	CVE-2022-23825	CVE-2022-2964	

Impacto

Vulnerabilidades de riesgo crítico

CVE-2022-30123: Vulnerabilidad que podría permitir un escape de shell en los componentes Lint y CommonLogger de Rack.

CVE-2021-21708: Vulnerabilidad que puede ser usada para liberar memoria designada, lo que puede llevar a corrupción de lotes. CVSS: 9.8.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

Juniper Networks Junos OS, todas las versiones.
Juniper Networks Junos OS Evolved, todas las versiones.
Juniper Networks Junos Space.

Enlaces

https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-QFX10000-Series-All-traffic-will-be-dropped-after-a-specific-valid-IP-packet-has-been-received-which-needs-to-be-routed-over-a-VXLAN-tunnel-CVE-2023-36835?language=en_US
https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-MX-Series-PFE-crash-upon-receipt-of-specific-packet-destined-to-an-AMS-interface-CVE-2023-36832?language=en_US
https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-The-l2cpd-will-crash-when-a-malformed-LLDP-packet-is-received-CVE-2023-36849?language=en_US
https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-SRX-Series-A-flowd-core-occurs-when-running-a-low-privileged-CLI-command-CVE-2023-36838?language=en_US
https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-SRX-Series-jbuf-memory-leak-when-SSL-Proxy-and-UTM-Web-Filtering-is-applied-CVE-2023-36831?language=en_US
https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-In-a-MoFRR-scenario-an-rpd-core-may-be-observed-when-a-low-privileged-CLI-command-is-executed-CVE-2023-36836?language=en_US
https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-The-FPC-will-crash-on-receiving-a-malformed-CFM-packet-CVE-2023-36848?language=en_US
https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-J-Web-Multiple-Vulnerabilities-in-PHP-software?language=en_US
https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-Evolved-Multiple-NTP-vulnerabilities-resolved
https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Multiple-vulnerabilities-have-been-resolved-in-MQTT
https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-SRX-4600-and-SRX-5000-Series-The-receipt-of-specific-genuine-packets-by-SRXes-configured-for-L2-transparency-will-cause-a-DoS-CVE-2023-36834
https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Contrail-Cloud-Multiple-Vulnerabilities-have-been-resolved-in-Contrail-Cloud-release-16-3-0

https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-SRX-Series-and-MX-Series-An-FPC-core-is-observed-when-IDP-is-enabled-on-the-device-and-a-specific-malformed-SSL-packet-is-received-CVE-2023-28985
https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-Space-Multiple-vulnerabilities-resolved-in-23-1R1-release
https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-An-rpd-crash-occurs-when-a-specific-L2VPN-command-is-run-CVE-2023-36840?language=en_US
https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-MX-Series-An-MPC-will-crash-upon-receipt-of-a-malformed-CFM-packet-CVE-2023-36850?language=en_US
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7653
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7654
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7655
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11358
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11868
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13817
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13946
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7071
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21702
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21703
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21704
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21705
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21707
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21708
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25220
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26401
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40085
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23825
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2588
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26373
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2795
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2964
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29900
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29901
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30123
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31625
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31626
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31627

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31628
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31629
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3276
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38023
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41974
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42703
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42898
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-4378
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36835
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36838
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36849

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.07.13 12:11:05 -04'00'