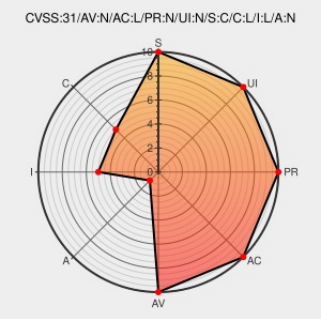
CVE-2023-28971

Published on: Not Yet Published

Last Modified on: 04/27/2023 07:54:00 PM UTC

CVE-2023-28971 - advisory for JSA70595

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Paragon Active Assurance from Juniper contain the following vulnerability:

An Improper Restriction of Communication Channel to Intended Endpoints vulnerability in the timescaledb feature of Juniper Networks Paragon Active Assurance (PAA) (Formerly Netrounds) allows an attacker to bypass existing firewall rules and limitations used to restrict internal communcations. The Test Agents (TA) Appliance connects to the Control Center (CC) using OpenVPN. TA's are assigned an internal IP address in the 100.70.0.0/16 range. Firewall rules exists to limit communication from TA's to the CC to specific services only. OpenVPN is configured to not allow direct communication between Test Agents in the OpenVPN application itself, and routing is normally not enabled on the server running the CC application. The timescaledb feature is installed as an optional package on the Control Center. When the timescaledb container is started, this causes side-effects by bypassing the existing firewall rules and limitations for Test Agent communications. Note: This issue only affects customers hosting their own on-prem Control Center. The Paragon Active Assurance Software as a Service (SaaS) is not affected by this vulnerability since the timescaledb service is not enabled. This issue affects all on-prem versions of Juniper Networks Paragon Active Assurance prior to 4.1.2.

CVE-2023-28971 has been assigned by sirt@juniper.net to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Juniper Networks** - **Paragon Active Assurance** version **< 4.1.2**

Vulnerability Patch/Work Around

If the timescaledb feature is not used - disable the service and disable IP forwarding. root@ncc:~# systemctl stop netrounds-timescaledb root@ncc:~# systemctl disable netrounds-timescaledb root@ncc:~# echo 0 > /proc/sys/net/ipv4/ip_forward In case timescaledb feature is used - drop forwarded packets by changing default forward policy to drop packets: Stop running services, to clear dynamic rules ncc services stop openvpn metrics timescaledb Set default DROP policy for forwarding iptables -P FORWARD DROP ip6tables -P FORWARD DROP Install iptables-persistent and save rules apt-get install iptables-persistent iptables-save > /etc/iptables/rules.v4 ip6tables-save > /etc/iptables/rules.v6 Restart services ncc services start openvpn metrics timescaledb

CVSS3 Score: 7.2 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVE References

Description	Tags	Link
CEC Juniper Community	supportportal.juniper.net text/html	CONFIRM supportportal.juniper.net/JSA70595

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Juniper	Paragon Active Assurance	All	All	All	All

cpe:2.3:a:juniper:paragon_active_assurance:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@RedPacketSec	Juniper Networks Paragon Active Assurance security bypass | CVE-2023-28971 - redpacketsecurity.com/juniper-networ… #CVE… twitter.com/i/web/status/1…	2023-04-13 09:05:39
@CVEreport	CVE-2023-28971 : An Improper Restriction of Communication Channel to Intended Endpoints vulnerability in the timesc… twitter.com/i/web/status/1…	2023-04-17 21:23:21

← Previous ID

Next ID→