



CVE-2021-31376

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-31376
State	PUBLIC
Assigner	sirt@juniper.net
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-10-19 19:15:00 UTC
Updated	2021-10-25 16:20:00 UTC
Description	An Improper Input Validation vulnerability in Packet Forwarding Engine manager (FXPC) process of Juniper Networks Junos

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Juniper	Acx1000	-	All	All	All
Hardware	Juniper	Acx1100	-	All	All	All
Hardware	Juniper	Acx2100	-	All	All	All
Hardware	Juniper	Acx2200	-	All	All	All
Hardware	Juniper	Acx4000	-	All	All	All
Hardware	Juniper	Acx500	-	All	All	All
Hardware	Juniper	Acx5048	-	All	All	All
Hardware	Juniper	Acx5096	-	All	All	All
Operating System	Juniper	Junos	18.4	r3-s7	All	All

References

Reference

- 2021-10 Security Bulletin: Junos OS: ACX Series: Packet Forwarding Engine manager (FXPC) process crashes when processing DHCPv6 pa
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)