CVE-2019-0071

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2019-0071
State	PUBLIC
Assigner	sirt@juniper.net
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-09 20:15:00 UTC
Updated	2020-09-29 00:20:00 UTC
Description	Veriexec is a kernel-based file integrity subsystem in Junos OS that ensures only authorized binaries are able to be execute

Risk And Classification

Problem Types: CWE-354

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Juniper	Ex2300	-	All	All	All
Hardware	Juniper	Ex2300	-	All	All	All
Hardware	Juniper	Ex2300-c	-	All	All	All
Hardware	Juniper	Ex2300-c	-	All	All	All
Hardware	Juniper	Ex3400	-	All	All	All
Hardware	Juniper	Ex3400	-	All	All	All
Operating System	Juniper	Junos	18.1	r3-s4	All	All
Operating System	Juniper	Junos	18.3	r1-s3	All	All
Operating System	Juniper	Junos	18.1	r3-s4	All	All
Operating System	Juniper	Junos	18.3	r1-s3	All	All

References

Reference
Veriexec Overview - TechLibrary - Juniper Networks
2019-10 Security Bulletin: Junos OS: EX2300, EX3400 Series: Veriexec signature checking not enforced in specific versions of Junos OS (CV
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**