



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 executed.

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 (CVE-2019-0071)
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](#).

Free CVE JSON API [cve.report/api](#)

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