



CVE-2023-28973

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

Summary

CVE	CVE-2023-28973
State	PUBLIC
Assigner	sirt@juniper.net
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-17 22:15:00 UTC
Updated	2023-04-28 14:24:00 UTC
Description	An Improper Authorization vulnerability in the 'sysmanctl' shell command of Juniper Networks Junos OS Evolved allows a local user to execute arbitrary commands with root privileges. The vulnerability is caused by a lack of proper authorization checks in the 'sysmanctl' command. An attacker can exploit this vulnerability by sending a specially crafted request to the 'sysmanctl' command, which will then execute the requested command with root privileges. This could allow an attacker to gain full control of the device.

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Juniper	Junos Os Evolved	All	All	All	All
Operating System	Juniper	Junos Os Evolved	20.4	-	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r1	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r1-s2	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r2	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r2-s1	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r2-s2	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r2-s3	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r3	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r3-s1	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r3-s2	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r3-s3	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r3-s4	All	All
Operating System	Juniper	Junos Os Evolved	21.1	-	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r1	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r1-s1	All	All

Operating System	Juniper	Junos Os Evolved	21.1	r2	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r3	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r3-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r3-s2	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r3-s3	All	All
Operating System	Juniper	Junos Os Evolved	21.2	-	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r1	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r1-s2	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r2	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r2-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r2-s2	All	All
Operating System	Juniper	Junos Os Evolved	21.3	-	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r1	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.4	-	All	All
Operating System	Juniper	Junos Os Evolved	21.4	r1	All	All
Operating System	Juniper	Junos Os Evolved	21.4	r1-s1	All	All

References

Reference	Source	Link	Tags
CEC Juniper Community	CONFIRM	supportportal.juniper.net	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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

