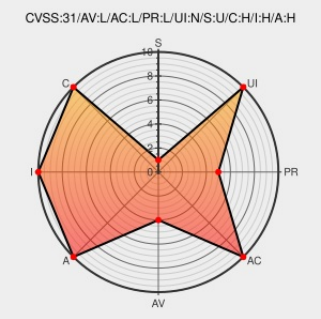
CVE-2022-22187

Published on: Not Yet Published

Last Modified on: 01/31/2023 06:04:00 PM UTC

CVE-2022-22187 - advisory for JSA69495

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



Certain versions of Identity Management Service from Juniper contain the following vulnerability:

An Improper Privilege Management vulnerability in the Windows Installer framework used in the Juniper Networks Juniper Identity Management Service (JIMS) allows an unprivileged user to trigger a repair operation. Running a repair operation, in turn, will trigger a number of file operations in the %TEMP% folder of the user triggering the repair. Some of these operations will be performed from a SYSTEM context (started via the Windows Installer service), including the execution of temporary files. An attacker may be able to provide malicious binaries to the Windows Installer, which will be executed with high privilege, leading to a local privilege escalation. This issue affects Juniper Networks Juniper Identity Management Service (JIMS) versions prior to 1.4.0.

CVE-2022-22187 has been assigned by sirt@juniper.net to track the vulnerability - currently rated as HIGH severity.

Juniper SIRT is not aware of any malicious exploitation of this vulnerability.

Affected Vendor/Software: **Juniper Networks** - **Juniper Identity Management Service (JIMS)** version **< 1.4.0**

Vulnerability Patch/Work Around

There are no viable workarounds for this issue.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Vulnerability-Disclosures/MNDT-2022-0029.md at master · mandiant/Vulnerability-Disclosures · GitHub	github.com text/html	MISC github.com/mandiant/Vulnerability-Disclosures/blob/master/2022/MNDT-2022-0029/MNDT-2022-0029.md
CEC Juniper Community	kb.juniper.net text/html	CONFIRM kb.juniper.net/JSA69495

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Juniper	Identity Management Service	All	All	All	All

cpe:2.3:a:juniper:identity_management_service:*:*:*:*:*:windows:*:*:

Discovery Credit

Juniper SIRT would like to acknowledge and thank Ronnie Salomonsen from Mandiant for responsibly reporting this vulnerability.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-22187 : An Improper Privilege Management vulnerability in the #Windows Installer framework used in the Jun… twitter.com/i/web/status/1…	2022-04-14 15:56:00
/r/netcve	CVE-2022-22187	2022-04-14 16:38:44

← Previous ID

Next ID→

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