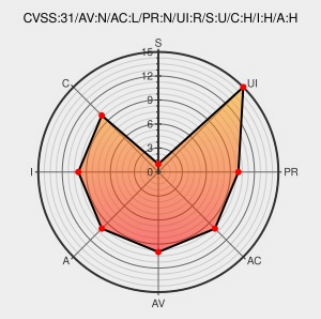
CVE-2020-15909

Published on: 10/19/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:41 PM UTC

CVE-2020-15909

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



Certain versions of N-central from Solarwinds contain the following vulnerability:

SolarWinds N-central through 2020.1 allows session hijacking and requires user interaction or physical access. The N-Central JSESSIONID cookie attribute is not checked against multiple sources such as sourceip, MFA claim, etc. as long as the victim stays logged in within N-Central. To take advantage of this, cookie could be stolen and the JSESSIONID can be captured. On its own this is not a surprising result; low security tools allow the cookie to roam from machine to machine. The JSESSION cookie can then be used on the attackers' workstation by browsing to the victim's NCentral server URL and replacing the JSESSIONID attribute value by the captured value. Expected behavior would be to check this against a second source and enforce at least a reauthentication or multi factor request as N-Central is a highly privileged service.

CVE-2020-15909 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
	Exploit Third Party Advisory limenetworks.nl application/pdf	MISC limenetworks.nl/wp-content/uploads/CVE-934261-v-1.2.pdf
MSP N-central | SolarWinds MSP	Product Vendor Advisory www.solarwindsmsp.com text/html	MISC www.solarwindsmsp.com/products/n-central

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Solarwinds	N-central	All	All	All	All

cpe:2.3:a:solarwinds:n-central:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→