



CVE-2020-7984

Published on: 01/26/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:53 PM UTC

CVE-2020-7984

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [N-central](#) from [Solarwinds](#) contain the following vulnerability:

SolarWinds N-central before 12.1 SP1 HF5 and 12.2 before SP1 HF2 allows remote attackers to retrieve cleartext domain admin credentials from the Agent & Probe settings, and obtain other sensitive information. The attacker can use a customer ID to self register and read any aspects of the agent/appliance configuration.

CVE-2020-7984 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Security News Bot on Twitter: "SolarWindows MSP n-Central Information #Disclosure https://t.co/O0VixVfX8s #PacketStorm"	Third Party Advisory nitter.domain.glass text/html	MISC twitter.com/SecurityNewsbot/status/1219722631898812416

Validating the SolarWinds N-central "Dumpster Diver" Vulnerability	Exploit Patch Third Party Advisory blog.huntresslabs.com text/html	 MISC blog.huntresslabs.com/validating-the-solarwinds-n-central-dumpster-diver-vulnerability-5e3a045982e5
Solarwinds MSP Identity Server	Permissions Required Vendor Advisory community.solarwindsmisp.com text/html	 MISC community.solarwindsmisp.com/Support/Software-Downloads/MSP-N-Central/MSP-N-central-12-2-SP1-HF2
SolarWinds RMM Tool Has Open Zero-Day Exploit: Huntress Labs	Third Party Advisory www.crn.com text/html	 MISC www.crn.com/news/managed-services/solarwinds-rmm-tool-has-open-zero-day-exploit-huntress-labs
Solarwinds MSP Identity Server	Permissions Required Vendor Advisory community.solarwindsmisp.com text/html	 MISC community.solarwindsmisp.com/Support/Software-Downloads/MSP-N-Central/MSP-N-central-12-1-SP1-HF5
No Results Found ≈ Packet Storm	Broken Link Third Party Advisory VDB Entry packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/156033
How to Expunge credentials for Customer levels of SolarWinds N-central	Patch Vendor Advisory success.solarwindsmisp.com text/html	 MISC success.solarwindsmisp.com/kb/solarwinds_n-central/How-to-Expunge-credentials-for-Customer-levels-of-SolarWinds-N-central
	Third Party Advisory github.com text/plain Inactive Link Not Archived	 MISC github.com/flipflopfpv

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
Application	Solarwinds	N-central	All	All	All	All
cpe:2.3:a:solarwinds:n-central:*****:						
cpe:2.3:a:solarwinds:n-central:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#).

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