



CVE-2022-47508

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

Summary

CVE	CVE-2022-47508
State	PUBLIC
Assigner	psirt@solarwinds.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-15 19:15:00 UTC
Updated	2023-02-24 18:46:00 UTC
Description	Customers who had configured their polling to occur via Kerberos did not expect NTLM Traffic on their environment, but sin

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Solarwinds	Server And Application Monitor	2022.4	All	All	All

References

Reference	Source	Link	Tags
SolarWinds Trust Center Security Advisories CVE-2022-47508	MISC	www.solarwinds.com	
SAM 2023.1 Release Notes	MISC	documentation.solarwinds.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: SolarWinds would like to thank Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative for reporting on the issue in a responsible manner.

There are currently no legacy QID mappings associated with this CVE.

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