



CVE-2021-39274

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

Summary

CVE	CVE-2021-39274
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-19 12:15:00 UTC
Updated	2021-08-30 11:29:00 UTC
Description	In XeroSecurity Sn1per 9.0 (free version), insecure directory permissions (0777) are set during installation, allowing an unp

Risk And Classification

Problem Types: CWE-276

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xerosecurity	Sn1per	9.0	All	All	All

References

Reference
Insecure permissions (777) on installation directory after running install script allow code execution/privilege escalation. · Issue #357 · 1N3/Sn1per · GitHub
GitHub - nikip72/CVE-2021-39273-CVE-2021-39274: Two security issues identified in Sn1per v9.0 free version by XeroSecurity
Releases · 1N3/Sn1per · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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