



CVE-2020-11081

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

Summary

CVE	CVE-2020-11081
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-10 19:15:00 UTC
Updated	2023-01-20 20:32:00 UTC
Description	osquery before version 4.4.0 enables a privilege escalation vulnerability. If a Window system is configured with a PATH tha

Risk And Classification

Problem Types: CWE-114

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linuxfoundation	Osquery	All	All	All	All
Application	Linuxfoundation	Osquery	All	All	All	All

References

Reference	Source	
Disable openssl compression support (#6433) · osquery/osquery@4d4957f · GitHub	MISC	View
Release 4.4.0 · osquery/osquery · GitHub	MISC	View
Disable openssl compression support by Smjert · Pull Request #6433 · osquery/osquery · GitHub	MISC	View
osquery susceptible to DLL search order hijacking of zlib1.dll · Advisory · osquery/osquery · GitHub	CONFIRM	View
Privilege Escalation Bug in Osquery 4.2.0 (windows) via Dll Search Order Hijacking · Issue #6426 · osquery/osquery · GitHub	MISC	View
CVE Program record	CVE.ORG	View
NVD vulnerability detail	NVD	View

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

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](#)