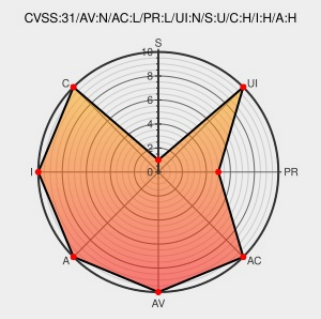
CVE-2023-31127

Published on: Not Yet Published

Last Modified on: 05/15/2023 06:08:00 PM UTC

CVE-2023-31127 - advisory for GHSA-qw76-4v8p-xq9f

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



Certain versions of Libspdm from Dmtf contain the following vulnerability:

libspdm is a sample implementation that follows the DMTF SPDM specifications. A vulnerability has been identified in SPDM session establishment in libspdm prior to version 2.3.1. If a device supports both DHE session and PSK session with mutual authentication, the attacker may be able to establish the session with `KEY_EXCHANGE` and `PSK_FINISH` to bypass the mutual authentication. This is most likely to happen when the Requester begins a session using one method (DHE, for example) and then uses the other method's finish (PSK_FINISH in this example) to establish the session. The session hashes would be expected to fail in this case, but the condition was not detected. This issue only impacts the SPDM responder, which supports `KEY_EX_CAP=1 and `PSK_CAP=10b` at same time with mutual authentication requirement. The SPDM requester is not impacted. The SPDM responder is not impacted if `KEY_EX_CAP=0` or `PSK_CAP=0` or `PSK_CAP=01b`. The SPDM responder is not impacted if mutual authentication is not required. libspdm 1.0, 2.0, 2.1, 2.2, 2.3 are all impacted. Older branches are not maintained, but users of the 2.3 branch may receive a patch in version 2.3.2. The SPDM specification (DSP0274) does not contain this vulnerability.

CVE-2023-31127 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **DMTF** - **libspdm** version **= < 2.3.2**

CVSS3 Score: 8.8 - HIGH

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

CVE References

Description	Tags	Link
Add handshake mode switch check in FINISH and PSK_FINISH. by jyao1 · Pull Request #2006 · DMTF/libspdm · GitHub	github.com text/html	MISC github.com/DMTF/libspdm/pull/2006
DMTF-2023-0001: SPDM mutual authentication bypass · Advisory · DMTF/libspdm · GitHub	github.com text/html	MISC github.com/DMTF/libspdm/security/advisories/GHSA-qw76-4v8p-xq9f
Add handshake mode switch check in FINISH and PSK_FINISH. by jyao1 · Pull Request #2007 · DMTF/libspdm · GitHub	github.com text/html	MISC github.com/DMTF/libspdm/pull/2007

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dmtf	Libspdm	All	All	All	All

cpe:2.3:a:dmtf:libspdm:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-31127 : libspdm is a sample implementation that follows the DMTF SPDM specifications. A vulnerability has… twitter.com/i/web/status/1…	2023-05-08 21:11:42

← Previous ID

Next ID→