DPDK- CVE-2022-28199

PUBLISHED: OCTOBER 3, 2022 | LAST UPDATE: OCTOBER 3, 2022

Summary

In August 2022, NVIDIA Corporation disclosed [1] a DPDK vulnerability that could allow a remote attacker to cause a denial or service or impact data integrity or confidentiality. This vulnerability could affect data plane services of ACOS devices deployed with Mellanox ConnectX-5 adapters and is addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2022-28199	CVSSv3	8.6 High	dpdk: error recovery in mlx5 driver not handled properly, allowing for denial of service [2]

Affected Releases

The table below indicates releases of ACOS exposed to this vulnerability and ACOS releases that address them. ACOS release families not indicated below are unaffected by these vulnerabilities.

Customers using affected ACOS releases can overcome vulnerability exposures by updating to the indicated resolved release. If the table does not list a corresponding resolved or unaffected release, then no ACOS release update is currently available.

Releases Affected			Releases Resolved or Unaffected
5.2.0	–	5.2.1-P5	5.2.1-P6

Workarounds and Mitigations

None

Software Updates

Software updates that address these vulnerabilities are or will be published at the following URL:

https://support.a10networks.com/

Vulnerability Details

The following table shares brief descriptions for the vulnerabilities addressed in this document.

Vulnerability ID	Description
CVE-2022-28199	NVIDIAs distribution of the Data Plane Development Kit (MLNX_DPDK) contains a vulnerability in the network stack, where error recovery is not handled properly, which can allow a remote attacker to cause denial of service and some impact to data integrity and confidentiality.

Related Links

Ref #	General Link
[1]	Security Bulletin: NVIDIA Data Plane Development Kit (MLNX_DPDK) - August 2022
[2]	NIST NVD, CVE-2022-28199

Acknowledgements

None

Modification History

Revision	Date	Description
1.0	2022-10-03	Initial Publication