



# CVE-2023-25522

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

## Summary

<b>CVE</b>	CVE-2023-25522
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@nvidia.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-07-04 00:15:00 UTC
<b>Updated</b>	2023-07-10 18:44:00 UTC
<b>Description</b>	NVIDIA DGX A100/A800 contains a vulnerability in SBIOS where an attacker may cause improper input validation by providing

## Risk And Classification

**Problem Types:** CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Nvidia</a>	<a href="#">Dgx A100</a>	-	All	All	All
Operating System	<a href="#">Nvidia</a>	<a href="#">Dgx A100 Firmware</a>	All	All	All	All
Hardware	<a href="#">Nvidia</a>	<a href="#">Dgx A800</a>	-	All	All	All
Operating System	<a href="#">Nvidia</a>	<a href="#">Dgx A800 Firmware</a>	All	All	All	All

## References

Reference	Source	Link	Tags
Security Bulletin: NVIDIA DGX A100 and DGX A800 - June 2023   NVIDIA	MISC	<a href="https://nvidia.custhelp.com">nvidia.custhelp.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)