# Details of your product

Below you may find the vulnerabilities for your product:

Product Name: nvidia nemo  
Product Version:   
  
Vulnerabilities:  
----------------------------------------------------------------------  
  
 CVE ID: CVE-2022-22821  
 Severity: Low  
 Description: NVIDIA NeMo before 1.6.0 contains a vulnerability in ASR WebApp, in which ../ Path Traversal may lead to deletion of any directory when admin privileges are available.  
 Mitigation: N/A  
 Published Date: 2022-01-10T08:42:55.693Z  
 Last Modified: 2024-11-21T01:17:31.133Z  
 URL: https://github.com/NVIDIA/NeMo/security/advisories/GHSA-rpx7-33j2-xx9x  
 ----------------------------------------------------------------------  
  
 CVE ID: CVE-2024-0081  
 Severity: High  
 Description: NVIDIA NeMo framework for Ubuntu contains a vulnerability in tools/asr\_webapp where an attacker may cause an allocation of resources without limits or throttling. A successful exploit of this vulnerability may lead to a server-side denial of service.  
 Mitigation: N/A  
 Published Date: 2024-04-05T13:45:07.033Z  
 Last Modified: 2024-11-21T03:15:51.183Z  
 URL: https://github.com/NVIDIA/NeMo/security/advisories/GHSA-x392-p65g-4rxx  
 ----------------------------------------------------------------------  
  
 CVE ID: CVE-2024-0129  
 Severity: Medium  
 Description: NVIDIA NeMo contains a vulnerability in SaveRestoreConnector where a user may cause a path traversal issue via an unsafe .tar file extraction. A successful exploit of this vulnerability may lead to code execution and data tampering.  
 Mitigation: N/A  
 Published Date: 2024-10-15T00:45:02.520Z  
 Last Modified: 2024-11-08T10:03:26.137Z  
 URL: https://nvidia.custhelp.com/app/answers/detail/a\_id/5580  
 ----------------------------------------------------------------------