



CVE-2021-41078

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

Summary

CVE	CVE-2021-41078
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-10-26 13:15:00 UTC
Updated	2021-10-29 01:34:00 UTC
Description	Nameko through 2.13.0 can be tricked into performing arbitrary code execution when deserializing the config file.

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nameko	Nameko	3.0.0	rc1	All	All
Application	Nameko	Nameko	3.0.0	rc2	All	All
Application	Nameko	Nameko	3.0.0	rc3	All	All
Application	Nameko	Nameko	3.0.0	rc4	All	All
Application	Nameko	Nameko	3.0.0	rc5	All	All
Application	Nameko	Nameko	3.0.0	rc6	All	All
Application	Nameko	Nameko	3.0.0	rc7	All	All
Application	Nameko	Nameko	3.0.0	rc8	All	All
Application	Nameko	Nameko	3.0.0	rc9	All	All
Application	Nameko	Nameko	All	All	All	All

References

Reference	Source	Link	Tags
Arbitrary code execution due to YAML deserialization · Advisory · nameko/nameko · GitHub	MISC	github.com	
GitHub - nameko/nameko: Python framework for building microservices	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980245 Python (pip) Security Update for nameko (GHSA-6p52-jr3q-c94g)

© [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](#)