



CVE-2019-15752

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

Summary

CVE	CVE-2019-15752
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-08-28 21:15:00 UTC
Updated	2023-11-07 03:05:00 UTC
Description	Docker Desktop Community Edition before 2.1.0.1 allows local users to gain privileges by placing a Trojan horse docker-c

Risk And Classification

EPSS: 0.493220000 probability, percentile 0.978210000 (date 2026-05-15)

CISA KEY: Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

Problem Types: CWE-732

CISA Known Exploited Vulnerability

Vendor	Docker
Product	Desktop Community Edition
Name	Docker Desktop Community Edition Privilege Escalation Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2019-15752

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Docker	Docker	All	All	All	All
Application	Docker	Docker	All	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

References

Reference	Source	Link	Tags
Elevation of Privilege in Docker for Windows by Morgan Roman Medium	MISC	medium.com	Exploit, Third Party Adv

Docker-Credential-Wincred.exe Privilege Escalation ≈ Packet Storm	MISC	packetstormsecurity.com	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!		lists.apache.org	
Elevation of Privilege in Docker for Windows by Morgan Roman Medium		medium.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[375594](#) Docker Desktop Community Local Privilege Escalation Vulnerability

© [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