



CVE-2019-5021

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

Summary

CVE	CVE-2019-5021
State	PUBLIC
Assigner	talos-cna@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-05-08 17:29:00 UTC
Updated	2022-06-13 18:45:00 UTC
Description	Versions of the Official Alpine Linux Docker images (since v3.3) contain a NULL password for the `root` user. This vulnerab

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Alpinelinux	Alpine Linux	-	All	All	All
Operating System	Alpinelinux	Alpine Linux	-	All	All	All
Application	F5	Big-ip Controller	1.2.1	All	All	All
Application	Gliderlabs	Docker-alpine	All	All	All	All
Application	Gliderlabs	Docker-alpine	All	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

References

Reference	Source	Link
[security-announce] openSUSE-SU-2019:1495-1: important: Recommended upda	SUSE	lists.opensuse.org
Alpine Linux Docker Image CVE-2019-5021 Hard Coded Credentials Authentication Bypass Vulnerability	BID	www.securityfocus.cc
support.f5.com/csp/article/K25551452	CONFIRM	support.f5.com
TALOS-2019-0782 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	talosintelligence.com
CVE-2019-5021 Alpine Linux Docker Image Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
Docker Image Vulnerability - CVE-2019-5021 Alpine Linux	MISC	alpinelinux.org
CVE Program record	CVE.ORG	www.cve.org

No vendor comments have been submitted for this CVE.

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

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)