CVE-2018-11764

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-11764
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-21 19:15:00 UTC
Updated	2022-06-03 18:57:00 UTC
Description	Web endpoint authentication check is broken in Apache Hadoop 3.0.0-alpha4, 3.0.0-beta1, and 3.0.0. Authenticated users

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Hadoop	3.0.0	-	All	All
Application	Apache	Hadoop	3.0.0	alpha4	All	All
Application	Apache	Hadoop	3.0.0	beta1	All	All
Application	Apache	Hadoop	3.0.0	-	All	All
Application	Apache	Hadoop	3.0.0	alpha4	All	All
Application	Apache	Hadoop	3.0.0	beta1	All	All

References

Reference	Source	Link	Tags
Pony Mail!	MISC	lists.apache.org	Mailing L
CVE-2018-11764 Apache Hadoop Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

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 registred 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