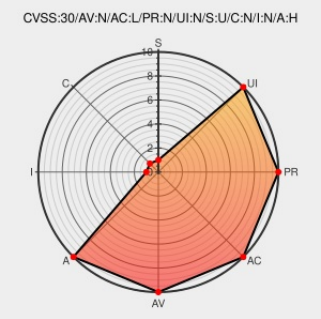
CVE-2018-17194

Published on: 12/19/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:19 PM UTC

CVE-2018-17194

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Nifi from Apache contain the following vulnerability:

When a client request to a cluster node was replicated to other nodes in the cluster for verification, the Content-Length was forwarded. On a DELETE request, the body was ignored, but if the initial request had a Content-Length value other than 0, the receiving nodes would wait for the body and eventually timeout. Mitigation: The fix to check DELETE requests and overwrite non-zero Content-Length header values was applied on the Apache NiFi 1.8.0 release. Users running a prior 1.x release should upgrade to the appropriate release.

CVE-2018-17194 has been assigned by security@apache.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Apache Software Foundation** - **Apache NiFi** version **Apache NiFi 1.0.0 - 1.7.1**

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Apache NiFi Security Reports	Vendor Advisory nifi.apache.org text/html	CONFIRM nifi.apache.org/security.html#CVE-2018-17194

Related QID Numbers

981333 Java (maven) Security Update for org.apache.nifi:nifi (GHSA-43fp-vwwg-qgv6)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Nifi	All	All	All	All

cpe:2.3:a:apache:nifi:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→