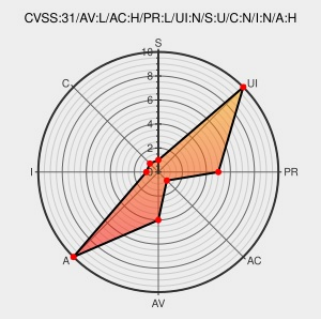
CVE-2019-3805

Published on: 05/03/2019 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:06:59 PM UTC

CVE-2019-3805

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



Certain versions of Jboss Enterprise Application Platform from Redhat contain the following vulnerability:

A flaw was discovered in wildfly versions up to 16.0.0.Final that would allow local users who are able to execute init.d script to terminate arbitrary processes on the system. An attacker could exploit this by modifying the PID file in /var/run/jboss-eap/ allowing the init.d script to terminate any process as root.

CVE-2019-3805 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Red Hat** - **wildfly** version **= affects up to 16.0.0.Final**

CVSS3 Score: 4.7 - MEDIUM

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

CVSS2 Score: 4.7 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Red Hat Customer Portal	Vendor Advisory	REDHAT RHSA-2019:1140

	access.redhat.com text/html	
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2019:1106
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2019:1107
May 2019 Wildfly Vulnerabilities in NetApp Products | NetApp Product Security	Third Party Advisory security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20190517-0004/
1660263 – (CVE-2019-3805) CVE-2019-3805 wildfly: Race condition on PID file allows for termination of arbitrary processes by local users	Issue Tracking Vendor Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3805
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2020:0727
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2019:1108
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2019:2413

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Jboss Enterprise Application Platform	6.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.0.0	All	All	All
Application	Redhat	Wildfly	All	All	All	All

cpe:2.3:a:redhat:jboss_enterprise_application_platform:6.0.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:7.0.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:6.0.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:7.0.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:wildfly:*:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-14317 : It was found that the issue for security flaw CVE-2019-3805 appeared again in a further version of… twitter.com/i/web/status/1…	2021-06-02 12:03:19

← Previous ID

Next ID→