Bug 1893070 (CVE-2020-25689) - CVE-2020-25689 wildfly-core: memory leak in WildFly host-controller in domain mode while not able to reconnect to domain-controller

Keywords: Security ×

Status: CLOSED ERRATA
Alias: CVE-2020-25689
Product: Security Response
Component: vulnerability
Version: unspecified
Hardware: All
OS: Linux
Priority: medium
Severity: medium
Target Milestone: ---
Assignee: Red Hat Product Security
QA Contact:
Docs Contact:
URL:
Whiteboard:
Depends On:
Blocks: 1891009
TreeView+ depends on / blocked

Reported: 2020-10-30 02:48 UTC by Ted Jongseok Won
Modified: 2022-10-02 21:48 UTC (History)
CC List: 57 users (show)
Fixed In Version:
Doc Type: ---
Doc Text: A memory leak flaw was found in WildFly in all versions up to 21.0.0.Final, where the host-controller tries to reconnect in a loop, generating new connections that are not properly closed while unable to connect to the domain controller. This flaw allows an attacker to cause an Out of memory (OOM) issue, leading to a denial of service. The highest threat from this vulnerability is to system availability.
Clone Of:
Environment:
Last Closed: 2021-01-25 16:47:03 UTC

Attachments (Terms of Use)

Add an attachment (proposed patch, testcase, etc.)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2021:0246	0	None	None	None	2021-01-25 16:29:08 UTC
Red Hat Product Errata	RHSA-2021:0247	0	None	None	None	2021-01-25 16:33:48 UTC
Red Hat Product Errata	RHSA-2021:0248	0	None	None	None	2021-01-25 16:38:37 UTC
Red Hat Product Errata	RHSA-2021:0250	0	None	None	None	2021-01-25 16:19:33 UTC
Red Hat Product Errata	RHSA-2021:0295	0	None	None	None	2021-02-08 09:06:58 UTC
Red Hat Product Errata	RHSA-2021:0327	0	None	None	None	2021-02-01 18:56:38 UTC
Red Hat Product Errata	RHSA-2022:5532	0	None	None	None	2022-07-07 14:20:01 UTC

Ted Jongseok Won 2020-10-30 02:48:54 UTC — Description

A memory leak flaw was found in WildFly in all versions up to 21.0.0.Final, where host-controller tries to reconnect in a loop, generating new connections which are not properly closed while not able to connect to domain-controller. This flaw allows an attacker to cause an Out of memory (OOM) issue, leading to a denial of service. The highest threat from this vulnerability is to system availability.

* Reference: https://issues.redhat.com/browse/WFCORE-5105
* Upstream patch: https://github.com/wildfly/wildfly-core/pull/4308
* Affected artifacts:
wildfly-host-controller-VERSION.jar
wildfly-protocol-VERSION.jar
jboss-cli-client.jar

Jonathan Christison 2020-11-02 17:38:25 UTC — Comment 6

This vulnerability is out of security support scope for the following products:
 * Red Hat JBoss Fuse 6

Please refer to https://access.redhat.com/support/policy/updates/jboss_notes for more details.

errata-xmlrpc 2021-01-25 16:19:30 UTC — Comment 10

This issue has been addressed in the following products:

  Red Hat JBoss Enterprise Application Platform

Via RHSA-2021:0250 https://access.redhat.com/errata/RHSA-2021:0250

errata-xmlrpc 2021-01-25 16:29:03 UTC — Comment 11

This issue has been addressed in the following products:

  Red Hat JBoss Enterprise Application Platform 7.3 for RHEL 6

Via RHSA-2021:0246 https://access.redhat.com/errata/RHSA-2021:0246

errata-xmlrpc 2021-01-25 16:33:44 UTC Comment 12

This issue has been addressed in the following products:

Red Hat JBoss Enterprise Application Platform 7.3 for RHEL 7

Via RHSA-2021:0247 https://access.redhat.com/errata/RHSA-2021:0247

errata-xmlrpc 2021-01-25 16:39:15 UTC Comment 13

This issue has been addressed in the following products:

Red Hat JBoss Enterprise Application Platform 7.3 for RHEL 8

Via RHSA-2021:0248 https://access.redhat.com/errata/RHSA-2021:0248

Product Security DevOps Team 2021-01-25 16:47:03 UTC Comment 14

This bug is now closed. Further updates for individual products will be reflected on the CVE page(s):

https://access.redhat.com/security/cve/cve-2020-25689

errata-xmlrpc 2021-02-01 18:56:35 UTC Comment 15

This issue has been addressed in the following products:

Red Hat Single Sign-On 7.4.5

Via RHSA-2021:0327 https://access.redhat.com/errata/RHSA-2021:0327

errata-xmlrpc 2021-02-08 09:06:49 UTC Comment 16

This issue has been addressed in the following products:

Red Hat Openshift Application Runtimes

Via RHSA-2021:0295 https://access.redhat.com/errata/RHSA-2021:0295

errata-xmlrpc 2022-07-07 14:19:58 UTC Comment 17

This issue has been addressed in the following products:

Red Hat Fuse 7.11

Via RHSA-2022:5532 https://access.redhat.com/errata/RHSA-2022:5532