CVE-2020-25689

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-25689
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-02 21:15:00 UTC
Updated	2023-02-12 23:40:00 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

Risk And Classification

Problem Types: CWE-401

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Netapp	Oncommand Insight	-	All	All	All
Application	Netapp	Service Level Manager	-	All	All	All
Application	Redhat	Fuse	6.0.0	All	All	All
Application	Redhat	Fuse	6.0.0	All	All	All
Application	Redhat	Jboss Data Grid	7.0.0	All	All	All
Application	Redhat	Jboss Data Grid	7.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.0.0	All	All	All
Application	Redhat	Jboss Fuse	7.0.0	All	All	All
Application	Redhat	Jboss Fuse	7.0.0	All	All	All
Application	Redhat	Openshift Application Runtimes	-	All	All	All
Application	Redhat	Openshift Application Runtimes	-	All	All	All
Application	Redhat	Single Sign-on	7.0	All	All	All
Application	Redhat	Single Sign-on	7.0	All	All	All

Application	Redhat	Wildfly	All	All	All	All

References

Reference
1893070 – (CVE-2020-25689) CVE-2020-25689 wildfly-core: memory leak in WildFly host-controller in domain mode while not able to reconne
CVE-2020-25689 WildFly Vulnerability in NetApp Products | NetApp Product Security
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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