# CVE-2020-25644

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2020-25644 |
| **State** | PUBLIC |
| **Assigner** | secalert@redhat.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2020-10-06 14:15:00 UTC |
| **Updated** | 2022-11-07 19:54:00 UTC |
| **Description** | A memory leak flaw was found in WildFly OpenSSL in versions prior to 1.1.3.Final, where it removes an HTTP session. It m |

## Risk And Classification

**Problem Types:** CWE-401

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Netapp | Oncommand Insight | - | All | All | All |
| Application | Netapp | Oncommand Workflow Automation | - | All | All | All |
| Application | Netapp | Service Level Manager | - | All | All | All |
| Application | Redhat | Data Grid | 8.0 | All | All | All |
| Application | Redhat | Data Grid | 8.0 | All | All | All |
| Application | Redhat | Jboss Data Grid | 7.0 | All | All | All |
| Application | Redhat | Jboss Data Grid | 7.0 | 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 Openssl | All | All | All | All |
| Application | Redhat | Wildfly Openssl | All | All | All | All |

## References

| Reference | Source |
|---|---|
| Login server redirect | MISC |
| CVE-2020-25644 WildFly Vulnerability in NetApp Products \| NetApp Product Security | CONFIRM |
| 1885485 – (CVE-2020-25644) CVE-2020-25644 wildfly-openssl: memory leak per HTTP session creation in WildFly OpenSSL | MISC |
| WFSSL-51 sessions not removed correctly by stuartwdouglas · Pull Request #4 · wildfly-security/wildfly-openssl-natives · GitHub | MISC |
| CVE Program record | CVE.ORG |
| NVD vulnerability detail | NVD |

No vendor comments have been submitted for this CVE.

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