# CVE-2020-10727

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2020-10727 |
| **State** | PUBLIC |
| **Assigner** | secalert@redhat.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2020-06-26 16:15:00 UTC |
| **Updated** | 2021-09-21 17:05:00 UTC |
| **Description** | A flaw was found in ActiveMQ Artemis management API from version 2.7.0 up until 2.12.0, where a user inadvertently store |

## Risk And Classification

**Problem Types:** CWE-312 | CWE-522

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Apache | Activemq Artemis | All | All | All | All |
| Application | Netapp | Oncommand Workflow Automation | - | All | All | All |

## References

| Reference | Source | Link |
|---|---|---|
| Login server redirect | MISC | issues.redhat.com |
| 1827200 – (CVE-2020-10727) CVE-2020-10727 broker: resetUsers operation stores password in plain text | CONFIRM | bugzilla.redhat.com |
| CVE-2020-10727 Apache ActiveMQ Artemis Vulnerability in NetApp Products \| NetApp Product Security | CONFIRM | security.netapp.com |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

No vendor comments have been submitted for this CVE.

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

**CVE.report and Source URL Uptime Status status.cve.report**