



# CVE-2019-0192

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2019-0192   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | security@apache.org   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2019-03-07 21:29:00 UTC   |
| <b>Updated</b>         | 2023-11-07 03:01:00 UTC   |
| <b>Description</b>     | In Apache Solr versions 5.0.0 to 5.5.5 and 6.0.0 to 6.6.5, the Config API allows to configure the JMX server via an HTTP PC |

## Risk And Classification

**Problem Types:** CWE-502

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                 | Product                                  | Version | Update | Edition | Language |
|-------------|------------------------|--|---------|--------|---------|----------|
| Application | <a href="#">Apache</a> | <a href="#">Solr</a>                     | All     | All    | All     | All      |
| Application | <a href="#">Apache</a> | <a href="#">Solr</a>                     | All     | All    | All     | All      |
| Application | <a href="#">Netapp</a> | <a href="#">Storage Automation Store</a> | -       | All    | All     | All      |
| Application | <a href="#">Netapp</a> | <a href="#">Storage Automation Store</a> | -       | All    | All     | All      |

## References

| Reference   | Source | Link  | Tags   |
|---|--------|---|--------|
| Pony Mail!  | MLIST  | <a href="https://lists.apache.org">lists.apache.org</a>                       |        |
| CVE-2019-0192 Deserialization of untrusted data via jmx.serviceUrl in Apache Solr | MLIST  | <a href="https://mail-archives.us.apache.org">mail-archives.us.apache.org</a> | Mailin |
| Pony Mail!  |        | <a href="https://lists.apache.org">lists.apache.org</a>                       |        |
| Pony Mail!  | MLIST  | <a href="https://lists.apache.org">lists.apache.org</a>                       | Mailin |
| Pony Mail!  | MLIST  | <a href="https://lists.apache.org">lists.apache.org</a>                       | Mailin |
| Pony Mail!  | MLIST  | <a href="https://lists.apache.org">lists.apache.org</a>                       | Mailin |
| Oracle Critical Patch Update Advisory - October 2020                              | MISC   | <a href="https://www.oracle.com">www.oracle.com</a>                           |        |
| Pony Mail!  |        | <a href="https://lists.apache.org">lists.apache.org</a>                       |        |
| Pony Mail!  |        | <a href="https://lists.apache.org">lists.apache.org</a>                       |        |
| Oracle Critical Patch Update - July 2019  | MISC   | <a href="https://www.oracle.com">www.oracle.com</a>                           |        |

|  |  |         |   |         |
|--|--|---------|---|---------|
| Pony Mail!   |  |         | <a href="https://lists.apache.org">lists.apache.org</a>           |         |
| Pony Mail!   |  | MLIST   | <a href="https://lists.apache.org">lists.apache.org</a>           |         |
| Pony Mail!   |  |         | <a href="https://lists.apache.org">lists.apache.org</a>           |         |
| Pony Mail!   |  |         | <a href="https://lists.apache.org">lists.apache.org</a>           |         |
| Red Hat Customer Portal  |  | REDHAT  | <a href="https://access.redhat.com">access.redhat.com</a>         |         |
| Pony Mail!   |  | MLIST   | <a href="https://lists.apache.org">lists.apache.org</a>           |         |
| Pony Mail!   |  | MLIST   | <a href="https://lists.apache.org">lists.apache.org</a>           | Mailin  |
| Pony Mail!   |  |         | <a href="https://lists.apache.org">lists.apache.org</a>           |         |
| Pony Mail!   |  |         | <a href="https://lists.apache.org">lists.apache.org</a>           |         |
| Pony Mail!   |  | MLIST   | <a href="https://lists.apache.org">lists.apache.org</a>           | Mailin  |
| Apache Solr CVE-2019-0192 Deserialization Remote Code Execution Vulnerability        |  | BID     | <a href="https://www.securityfocus.com">www.securityfocus.com</a> | Third I |
| CVE-2017-3164 Apache Solr Vulnerability in NetApp Products   NetApp Product Security |  | CONFIRM | <a href="https://security.netapp.com">security.netapp.com</a>     | Third I |
| CVE Program record   |  | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>                     | canon   |
| NVD vulnerability detail   |  | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                   | canon   |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980790 Java (maven) Security Update for org.apache.solr:solr-core (GHSA-xhcq-fv7x-grr2)

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**