



CVE-2021-29943

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2021-29943 |
| State | PUBLIC |
| Assigner | security@apache.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-04-13 07:15:00 UTC |
| Updated | 2021-06-08 13:51:00 UTC |
| Description | When using ConfigurableInternodeAuthHadoopPlugin for authentication, Apache Solr versions prior to 8.8.2 would forward/ |

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|------------------------|----------------------|---------|--------|---------|----------|
| Application | Apache | Solr | All | All | All | All |

References

| Reference | Source | Link | Tags |
|---|---------|---|---------------------|
| April 2021 Apache Solr Vulnerabilities in NetApp Products NetApp Product Security | CONFIRM | security.netapp.com | |
| Pony Mail! | MISC | lists.apache.org | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

Vendor Comments And Credit

Discovery Credit

LEGACY: Geza Nagy

Legacy QID Mappings

[982329](#) Java (maven) Security Update for org.apache.solr:solr-parent (GHSA-vf7p-j8x6-xvwp)

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)