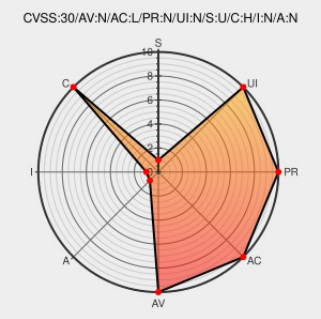
CVE-2017-3163

Published on: 08/30/2017 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:44:00 AM UTC

CVE-2017-3163

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Solr from Apache contain the following vulnerability:

When using the Index Replication feature, Apache Solr nodes can pull index files from a master/leader node using an HTTP API which accepts a file name. However, Solr before 5.5.4 and 6.x before 6.4.1 did not validate the file name, hence it was possible to craft a special request involving path traversal, leaving any file readable to the Solr server process exposed. Solr servers protected and restricted by firewall rules and/or authentication would not be at risk since only trusted clients and users would gain direct HTTP access.

CVE-2017-3163 has been assigned by security@apache.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Apache Software Foundation** - **Apache Solr** version **1.4.0 to 5.5.3**

Affected Vendor/Software: **Apache Software Foundation** - **Apache Solr** version **6.0.0 to 6.4.0**

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2018:1451
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2018:1449
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2018:1450
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2018:1448
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	MLIST [solr-user] 20170215 [SECURITY] CVE-2017-3163 Apache Solr ReplicationHandler path traversal attack
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2018:1447
Debian -- Security Information -- DSA-4124-1 lucene-solr	www.debian.org Depreciated Link text/html	DEBIAN DSA-4124

Related QID Numbers

981393 Java (maven) Security Update for org.apache.solr:solr-core (GHSA-387v-84cv-9qmc)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Solr	6.0.0	All	All	All
Application	Apache	Solr	6.0.1	All	All	All
Application	Apache	Solr	6.1.0	All	All	All
Application	Apache	Solr	6.2.0	All	All	All
Application	Apache	Solr	6.2.1	All	All	All
Application	Apache	Solr	6.3.0	All	All	All
Application	Apache	Solr	6.4.0	All	All	All
Application	Apache	Solr	6.0.0	All	All	All
Application	Apache	Solr	6.0.1	All	All	All
Application	Apache	Solr	6.1.0	All	All	All
Application	Apache	Solr	6.2.0	All	All	All
Application	Apache	Solr	6.2.1	All	All	All

Application	Apache	Solr	6.3.0	All	All	All
Application	Apache	Solr	6.4.0	All	All	All
Application	Apache	Solr	All	All	All	All

cpe:2.3:a:apache:solr:6.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:solr:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:solr:6.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:solr:6.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:solr:6.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:solr:6.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:solr:6.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:solr:6.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:solr:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:solr:6.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:solr:6.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:solr:6.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:solr:6.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:solr:6.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:solr:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→