SolrVulnerabilities

THIS PAGE IS OBSOLETE

This page has been superseded by SolrSecurity.

General and well-known vulnerabilities

Because Solr is a Java application that runs in an application server, it is rare for a security vulnerability to be found in Solr itself. When a vulnerability is found, it is almost always in either the JVM (java virtual machine) or the servlet container.

Heartbleed

✓ Solr is not directly vulnerable to the Heartbleed exploit, a security vulnerability in specific versions of OpenSSL.

Solr itself contains no SSL code. Whether or not the overall installation is vulnerable depends on a few factors. To be vulnerable, all of the following must be true: 1) The servlet container that runs Solr must have SSL enabled. 2) The JVM or the servlet container must use a vulnerable version of OpenSSL.

✓ If an installation uses the official Oracle JRE or JDK as the java virtual machine and Jetty or Tomcat as the servlet container, it is NOT vulnerable. The servlet container included in the Solr download is a stripped-down version of Jetty.

⚠ A vulnerability in other java virtual machines and servlet containers is unlikely, but please check with the software vendor to be sure.

⚠ If SSL for Solr is handled by other software or hardware (HTTP proxies in particular), that hardware or software may be using a vulnerable version of OpenSSL. Check with the vendor to be sure.

Vulnerabilities specific to Solr

This section has no available information at this time.