



CVE-2019-17558

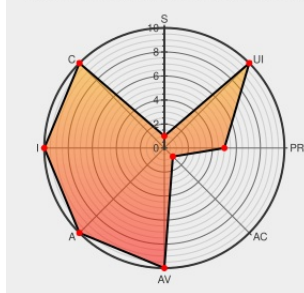
Published on: 12/30/2019 12:00:00 AM UTC

Last Modified on: 02/20/2022 06:42:00 AM UTC

CVE-2019-17558

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Solr](#) from [Apache](#) contain the following vulnerability:

Apache Solr 5.0.0 to Apache Solr 8.3.1 are vulnerable to a Remote Code Execution through the VelocityResponseWriter. A Velocity template can be provided through Velocity templates in a configset `velocity/` directory or as a parameter. A user defined configset could contain renderable, potentially malicious, templates. Parameter provided templates are disabled by default, but can be enabled by

setting `params.resource.loader.enabled` by defining a response writer with that setting set to `true`. Defining a response writer requires configuration API access. Solr 8.4 removed the params resource loader entirely, and only enables the configset-provided template rendering when the configset is `trusted` (has been uploaded by an authenticated user).

CVE-2019-17558 has been assigned by security@apache.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **4.6 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [lucene-issues] 20200113 [GitHub] [lucene-solr] Sachpat closed pull request #1156: SOLR-13971: CVE-2019-17558: Velocity custom template RCE vulnerability
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [lucene-solr-user] 20210203 Re: SolrCloud keeps crashing
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [submarine-commits] 20201209 [GitHub] [submarine] QiAnXinCodeSafe opened a new issue #474: There is a vulnerability in Apache Solr 5.5.4,upgrade recommended
Pony Mail!	Mailing List Patch Vendor Advisory lists.apache.org text/html	 MLIST [lucene-issues] 20200107 [jira] [Commented] (SOLR-13971) CVE-2019-17558: Velocity custom template RCE vulnerability
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [lucene-issues] 20200113 [GitHub] [lucene-solr] chatman commented on issue #1156: SOLR-13971: CVE-2019-17558: Velocity custom template RCE vulnerability
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [lucene-dev] 20200213 Re: 7.7.3 bugfix release
Pony Mail!	Mailing List Patch Vendor Advisory lists.apache.org text/html	 MLIST [lucene-dev] 20200214 Re: 7.7.3 bugfix release
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [lucene-issues] 20200219 [jira] [Updated] (SOLR-14025) CVE-2019-17558: Velocity response writer RCE vulnerability persists after 8.3.1
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [lucene-issues] 20200108 [GitHub] [lucene-solr] Sachpat opened a new pull request #1156: SOLR-13971
Apache Solr 8.3.0 Velocity Template Remote Code Execution ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/157078/Apache-Solr-8.3.0-Velocity-Template-Remote-Code-Execution.html
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [lucene-issues] 20200108 [GitHub] [lucene-solr] artem-smotrakov commented on a change in pull request #1156: SOLR-13971: CVE-2019-17558: Velocity custom template RCE vulnerability
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [lucene-issues] 20210210 [GitHub] [lucene-solr] rhtham edited a comment on pull request #1156: SOLR-13971: CVE-2019-17558: Velocity custom template RCE vulnerability
Oracle Critical Patch Update Advisorv - October 2020	Third Party Advisory www.oracle.com	 MISC www.oracle.com/security-alerts/cpuoct2020.html

Pony Mail!	Mailing List text/html	
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [ambari-issues] 20200220 [jira] [Created] (AMBARI-25482) solr dependence CVE-2019-17558
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [lucene-issues] 20200108 [GitHub] [lucene-solr] Sachpat commented on issue #1156: SOLR-13971: CVE-2019-17558: Velocity custom template RCE vulnerability
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [lucene-solr-user] 20210212 CVE-2019-17558 on SOLR 6.1
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [lucene-solr-user] 20200320 Re: CVEs (vulnerabilities) that apply to Solr 8.4.1
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [lucene-issues] 20200108 [jira] [Commented] (SOLR-13971) CVE-2019-17558: Velocity custom template RCE vulnerability
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [lucene-issues] 20200113 [GitHub] [lucene-solr] Sachpat commented on issue #1156: SOLR-13971: CVE-2019-17558: Velocity custom template RCE vulnerability
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [lucene-issues] 20200108 [jira] [Updated] (SOLR-14025) CVE-2019-17558: Velocity response writer RCE vulnerability persists after 8.3.1
Pony Mail!	Mailing List Patch Vendor Advisory lists.apache.org text/html	 MLIST [lucene-issues] 20200113 [jira] [Commented] (SOLR-14025) CVE-2019-17558: Velocity response writer RCE vulnerability persists after 8.3.1
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [lucene-issues] 20210315 [GitHub] [lucene-solr] erikhatcher commented on pull request #1156: SOLR-13971: CVE-2019-17558: Velocity custom template RCE vulnerability
[SOLR-13971] Velocity custom template RCE vulnerability - ASF JIRA	Exploit Issue Tracking Patch Vendor Advisory issues.apache.org text/html	 MISC issues.apache.org/jira/browse/SOLR-13971
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [lucene-issues] 20210210 [GitHub] [lucene-solr] rtham commented on pull request #1156: SOLR-13971: CVE-2019-17558: Velocity custom template RCE vulnerability
Pony Mail!	Mailing List Vendor Advisory lists.apache.org text/html	 MLIST [lucene-solr-user] 20210213 Re: CVE-2019-17558 on SOLR 6.1
Pony Mail!	Mailing List Vendor Advisory	 MLIST [lucene-solr-user] 20200320 CVEs (vulnerabilities) that apply to Solr 8.4.1

lists.apache.org
[text/html](#)

Pony Mail!

lists.apache.org
[text/html](#)

 MLIST [druid-commits] 20210324 [GitHub] [druid] jihoonson opened a new pull request #11030: Suppress cves

Pony Mail!

[Mailing List](#)
[Vendor Advisory](#)
lists.apache.org
[text/html](#)

 MLIST [lucene-issues] 20200108 [GitHub] [lucene-solr] Sachpat commented on a change in pull request #1156: SOLR-13971: CVE-2019-17558: Velocity custom template RCE vulnerability

Pony Mail!

[Mailing List](#)
[Vendor Advisory](#)
lists.apache.org
[text/html](#)

 MLIST [lucene-solr-user] 20210212 Re: CVE-2019-17558 on SOLR 6.1

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[981952](#) Java (maven) Security Update for org.apache.solr:solr-core (GHSA-ww97-9w65-2crx)

Exploit/POC from Github

Solr_CVE-2019-17558

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Solr	All	All	All	All
Application	Oracle	Primavera Unifier	16.1	All	All	All
Application	Oracle	Primavera Unifier	16.2	All	All	All
Application	Oracle	Primavera Unifier	18.8	All	All	All
Application	Oracle	Primavera Unifier	19.12	All	All	All
Application	Oracle	Primavera Unifier	16.1	All	All	All
Application	Oracle	Primavera Unifier	16.2	All	All	All
Application	Oracle	Primavera Unifier	18.8	All	All	All
Application	Oracle	Primavera Unifier	19.12	All	All	All
Application	Oracle	Primavera Unifier	All	All	All	All

[cpe:2.3:a:apache:solr:*****:*](#)

[cpe:2.3:a:oracle:primavera_unifier:16.1:*****:*](#)

[cpe:2.3:a:oracle:primavera_unifier:16.2:*****:*](#)

[cpe:2.3:a:oracle:primavera_unifier:18.8:*****:*](#)

cpe:2.3:a:oracle:primavera_unifier:19.12:*:*:*:*:*:
cpe:2.3:a:oracle:primavera_unifier:16.1:*:*:*:*:*:
cpe:2.3:a:oracle:primavera_unifier:16.2:*:*:*:*:*:
cpe:2.3:a:oracle:primavera_unifier:18.8:*:*:*:*:*:
cpe:2.3:a:oracle:primavera_unifier:19.12:*:*:*:*:*:
cpe:2.3:a:oracle:primavera_unifier:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
← Previous ID Next ID→		