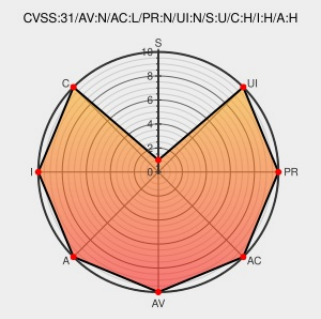
CVE-2018-17200

Published on: 09/11/2019 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:54:00 AM UTC

CVE-2018-17200

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



Certain versions of Ofbiz from Apache contain the following vulnerability:

The Apache OFBiz HTTP engine (org.apache.ofbiz.service.engine.HttpEngine.java) handles requests for HTTP services via the /webtools/control/httpService endpoint. This service takes the `serviceContent` parameter in the request and deserializes it using XStream. This `XStream` instance is slightly guarded by disabling the creation of `ProcessBuilder`. However, this can be easily bypassed (and in multiple ways). Mitigation: Upgrade to 16.11.06 or manually apply the following commits on branch 16 r1850017+1850019

CVE-2018-17200 has been assigned by security@apache.org to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Apache** - **OFBiz** version **OFBiz 16.11.01 to 16.11.05**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Pony Mail!	lists.apache.org text/html	MLIST [ofbiz-commits] 20200306 svn commit: r1874880 [5/5] - in /ofbiz/site: download.html release-notes-17.12.01.html security.html template/page/download.tpl.php template/page/release-notes-17.12.01.tpl.php template/page/security.tpl.php
Pony Mail!	lists.apache.org text/html	MLIST [ofbiz-commits] 20200430 [ofbiz-site] branch master updated: Update for 2 last CVEs: CVE-2019-0235 & CVE-2019-12425
Pony Mail!	lists.apache.org text/html	MLIST [ofbiz-commits] 20200430 svn commit: r1877207 - in /ofbiz/site: security.html template/page/security.tpl.php
Pony Mail!	lists.apache.org text/html	MLIST [ofbiz-commits] 20200206 svn commit: r1873710 - in /ofbiz/site: security.html template/page/security.tpl.php
Pony Mail!	Mailing List Vendor Advisory s.apache.org text/html	MLIST [ofbiz-dev] 20190910 [CVE-2018-17200] Apache OFBiz unauthenticated remote code execution vulnerability in HttpEngine

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Ofbiz	All	All	All	All

cpe:2.3:a:apache:ofbiz:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→