



CVE-2011-3600

Published on: 11/25/2019 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:32:00 AM UTC

CVE-2011-3600

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

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

The `/webtools/control/xmlrpc` endpoint in OFBiz XML-RPC event handler is exposed to External Entity Injection by passing DOCTYPE declarations with executable payloads that discloses the contents of files in the filesystem. In addition, it can also be used to probe for open network ports, and figure out from returned error messages whether a file exists or not. This affects OFBiz 16.11.01 to 16.11.04.

CVE-2011-3600 has been assigned by [secalert@redhat.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **OFBiz** - **OFBiz** version = **16.11.01 to 16.11.04**

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
-------------	------	------

705869 – (CVE-2011-3600) CVE-2011-3600 XML-RPC SAX parser information exposure	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	 MISC bugzilla.redhat.com/show_bug.cgi?id=CVE-2011-3600
[SECURITY] CVE-2011-3600 Apache OFBiz XML-RPC XXE Vulnerability	Exploit Mailing List Vendor Advisory mail-archives.apache.org text/xml	 MISC mail-archives.apache.org/mod_mbox/ofbiz-user/201810.mbox/%3Cfad45546-af86-0293-9ea7-014553474b30%40apache.org%3E
CVE-2011-3600	Third Party Advisory security-tracker.debian.org text/html	 MISC security-tracker.debian.org/tracker/CVE-2011-3600
CVE-2011-3600 - Red Hat Hat Customer Portal	Third Party Advisory access.redhat.com text/html	 MISC access.redhat.com/security/cve/cve-2011-3600
Pony Mail!	lists.apache.org text/html	 MISC lists.apache.org/thread.html/7793319ae80ec350f7b82a8763460944f120ebe447f14a12155d0550@

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.

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 →

[site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report