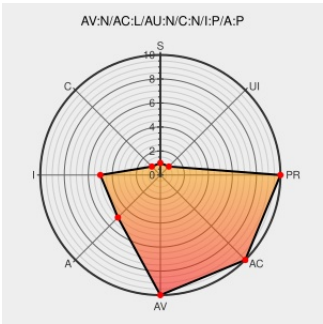
CVE-2016-0491

Published on: 01/20/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:14 PM UTC

CVE-2016-0491

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



Certain versions of Application Testing Suite from Oracle contain the following vulnerability:

Unspecified vulnerability in the Oracle Application Testing Suite component in Oracle Enterprise Manager Grid Control 12.4.0.2 and 12.5.0.2 allows remote attackers to affect integrity and availability via unknown vectors related to Load Testing for Web Apps. NOTE: the previous information is from the January 2016 CPU. Oracle has not commented on third-party claims that the UploadFileAction servlet allows remote authenticated users to upload and execute arbitrary files via an * (asterisk) character in the fileType parameter.

CVE-2016-0491 has been assigned by secalert_us@oracle.com to track the vulnerability

CVSS2 Score: 6.4 - MEDIUM

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

CVE References

Description	Tags	Link
Oracle Enterprise Manager Grid Control Multiple Flaws Let Remote and Local Users Access Data, Modify Data, and Deny Service - SecurityTracker	Third Party Advisory, VDB Entry, www.securitytracker.com, text/html	SECTRACK 1034734
Exim4 string_format Function Heap Buffer Overflow	Third Party Advisory, VDB Entry, www.rapid7.com, text/html	MISC www.rapid7.com/db/modules/exploit/multi/http/oracle_ats_file_upload
Oracle Enterprise Manager CVE-2016	Third Party Advisory	BID 81169

Oracle Enterprise Manager CVE-2016-0491 Remote Code Execution Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 81169
Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-16-047
Oracle Application Testing Suite (ATS) 12.4.0.2.0 - Authentication Bypass / Arbitrary File Upload - JSP webapps Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 39691
Oracle Application Testing Suite (ATS) - Arbitrary File Upload (Metasploit) - Java remote Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 39852
Oracle ATS Arbitrary File Upload ≈ Packet Storm	Exploit packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/137175/Oracle-ATS-Arbitrary-File-Upload.html
Oracle Critical Patch Update - January 2016	Patch Vendor Advisory www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Application Testing Suite	12.4.0.2	All	All	All
Application	Oracle	Application Testing Suite	12.5.0.2	All	All	All
Application	Oracle	Application Testing Suite	12.4.0.2	All	All	All
Application	Oracle	Application Testing Suite	12.5.0.2	All	All	All

cpe:2.3:a:oracle:application_testing_suite:12.4.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:application_testing_suite:12.5.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:application_testing_suite:12.4.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:application_testing_suite:12.5.0.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→