Vulnerability Report - JMX-Console in JBoss AS is vulnerable to attack

Unisys ID:	**UIS-2014-35**
Status:	Published
CVE-ID:	CVE-2010-0738
Affected Product:	MCP OSP or Notification Sevices servers
Affected Version:	07.2
Impact:	MEDIUM
CVSS v4.x Base Score:	
CVSS v4.x Vector:	Not Supplied **v4 Calculator**
CVSS v3.x Base Score:	5.0
CVSS v3.x Vector:	**(AV:N/AC:L/Au:N/C:P/I:N/A:N) v3 Calculator**
CVSS v2.0 Base Score:	
CVSS v2.0 Vector:	Not Supplied **v2 Calculator**
Common Weakness Enumeration (CWE):	
Common Platform Enumeration (CPE):	
Source:	Client Reported
Keyword(s):	JBOSS, OSP, NGNS, MCP, CVE-2010-0738

Vulnerability Description:

The JMX-Console web application in JBossAs in Red Hat JBoss Enterprise Application Platform (aka JBoss EAP or JBEAP) 4.2 before 4.2.0.CP09 and 4.3 before 4.3.0.CP08 performs access control only for the GET and POST methods, which allows remote attackers to send requests to this application's GET handler by using a different method.

System Configuration:

Any server running Linux RH Server with Notif-Services installed.

Impact of Exploiting Vulnerability:

See CVE for details.

Remediation Description:

Details for Remediation are available in PLE 19053890.

Workaround Information:

Details for Workaround are available in PLE 19053890.

References:

Additional Vendor Comment:

Disclaimer:

Unisys Corporation provides the information in this Security Vulnerability Report "AS IS." No warranties of any nature are extended by or for the information. Unisys disclaims any financial or other responsibility that may result from your use of the information, including direct, indirect, special, or consequential damages.

Paper copies are not controlled and may be out of date; reference the Product Support Web site for current data.