

# Security News

## 2011-21006 Cisco Unified Operations Manager Multiple Vulnerabilities

### **1. Affected Version**

Cisco Unified Operations Manager (CUOM) 8.0  
Cisco Unified Operations Manager (CUOM) 8.5

### **2. Description**

Multiple vulnerabilities have been reported in Cisco Unified Operations Manager (CUOM), which can be exploited by remote attacker to conduct cross-site scripting and SQL injection attacks.

### **3. Vulnerability Analysis**

The malicious script examples are listed as follows:

<pre>/iptm/advancedfind.do?extn=73fcb&lt;/script&gt;&lt;script&gt;alert(1)&lt;/script&gt;23fbe43447 /iptm/ddv.do? deviceInstanceName=f3806"%3balert(1)//9b92b050cf5&amp;deviceCapability=deviceCap /iptm/PRTTestCreation.do?RequestSource=dashboard&amp;MACs=&amp;CCMs='wait for %20delay'0:0:20'--&amp;Extns=&amp;IPs=</pre>
Table 1: The malicious script examples

The cross-site scripting vulnerability is due to improper validation of user-supplied input to certain scripts that make up the affected application. An unauthenticated, remote attacker could exploit this vulnerability by convincing a user to view a specially-crafted link. If successful, the attacker could conduct cross-site scripting attacks and gain access to sensitive information.

The attacker could also exploit SQL injection vulnerability by sending malicious requests to the targeted system. If successful, the attacker could execute arbitrary SQL code against the database underlying the affected application.

## **4. Recommendation**

1. AegisLab IDP signature database can prevent this attack since 19/05/2011.
2. Apply the appropriate patch for your system, as listed in [Cisco Security advisory](#).

## **5. Reference**

1. <http://tools.cisco.com/security/center/viewAlert.x?alertId=23085>
2. <http://tools.cisco.com/security/center/viewAlert.x?alertId=23086>
3. <http://tools.cisco.com/security/center/viewAlert.x?alertId=23087>
4. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0959>

**About Lionic:** Lionic Corporation is an innovative network security chip and IP design company. It provides optimal cost-performance solutions for network security products from 30Mbps SOHO devices to 4Gbps enterprise-level appliances.

**For more information, please visit Lionic website and contact our sales representatives.**

Web site: [www.lionic.com](http://www.lionic.com) e-mail: [sales@lionic.com](mailto:sales@lionic.com) Tel: 886-3-578-9399 Fax: 886-3-578-0707