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:

```
/iptm/advancedfind.do?extn=73fcb</script><script>alert(1)</script>23fbe43447
/iptm/ddv.do?
deviceInstanceName=f3806"%3balert(1)//9b92b050cf5&deviceCapability=deviceCap
/iptm/PRTestCreation.do?RequestSource=dashboard&MACs=&CCMs='waitfor
%20delay'0:0:20'--&Extns=&IPs=
```

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