



# CVE-2011-2738

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2011-2738
<b>State</b>	PUBLIC
<b>Assigner</b>	security_alert@emc.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2011-09-19 12:02:00 UTC
<b>Updated</b>	2018-10-09 19:32:00 UTC
<b>Description</b>	Multiple unspecified vulnerabilities in Cisco Unified Service Monitor before 8.6, as used in Unified Operations Manager before 8.6.

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Ciscoworks Lan Management Solution	3.0	All	All	All
Application	Cisco	Ciscoworks Lan Management Solution	3.0	december_2007	All	All
Application	Cisco	Ciscoworks Lan Management Solution	3.1	All	All	All
Application	Cisco	Ciscoworks Lan Management Solution	3.2	All	All	All
Application	Cisco	Ciscoworks Lan Management Solution	4.0	All	All	All
Application	Cisco	Ciscoworks Lan Management Solution	4.0.1	All	All	All
Application	Cisco	Ciscoworks Lan Management Solution	3.0	All	All	All
Application	Cisco	Ciscoworks Lan Management Solution	3.0	december_2007	All	All
Application	Cisco	Ciscoworks Lan Management Solution	3.1	All	All	All
Application	Cisco	Ciscoworks Lan Management Solution	3.2	All	All	All
Application	Cisco	Ciscoworks Lan Management Solution	4.0	All	All	All
Application	Cisco	Ciscoworks Lan Management Solution	4.0.1	All	All	All
Application	Cisco	Unified Operations Manager	1.0	All	All	All
Application	Cisco	Unified Operations Manager	1.1	All	All	All
Application	Cisco	Unified Operations Manager	2.0	All	All	All
Application	Cisco	Unified Operations Manager	2.0.1	All	All	All
Application	Cisco	Unified Operations Manager	2.0.2	All	All	All

Application	Cisco	Unified Operations Manager	2.0.3	All	All	All
Application	Cisco	Unified Operations Manager	2.1	All	All	All
Application	Cisco	Unified Operations Manager	2.2	All	All	All
Application	Cisco	Unified Operations Manager	2.3	All	All	All
Application	Cisco	Unified Operations Manager	8.0	All	All	All
Application	Cisco	Unified Operations Manager	1.0	All	All	All
Application	Cisco	Unified Operations Manager	1.1	All	All	All
Application	Cisco	Unified Operations Manager	2.0	All	All	All
Application	Cisco	Unified Operations Manager	2.0.1	All	All	All
Application	Cisco	Unified Operations Manager	2.0.2	All	All	All
Application	Cisco	Unified Operations Manager	2.0.3	All	All	All
Application	Cisco	Unified Operations Manager	2.1	All	All	All
Application	Cisco	Unified Operations Manager	2.2	All	All	All
Application	Cisco	Unified Operations Manager	2.3	All	All	All
Application	Cisco	Unified Operations Manager	8.0	All	All	All
Application	Cisco	Unified Operations Manager	All	All	All	All
Application	Cisco	Unified Service Monitor	1.1	All	All	All
Application	Cisco	Unified Service Monitor	2.0	All	All	All
Application	Cisco	Unified Service Monitor	2.0.1	All	All	All
Application	Cisco	Unified Service Monitor	2.1	All	All	All
Application	Cisco	Unified Service Monitor	2.2	All	All	All
Application	Cisco	Unified Service Monitor	2.3	All	All	All
Application	Cisco	Unified Service Monitor	8.0	All	All	All
Application	Cisco	Unified Service Monitor	1.1	All	All	All
Application	Cisco	Unified Service Monitor	2.0	All	All	All
Application	Cisco	Unified Service Monitor	2.0.1	All	All	All
Application	Cisco	Unified Service Monitor	2.1	All	All	All
Application	Cisco	Unified Service Monitor	2.2	All	All	All
Application	Cisco	Unified Service Monitor	2.3	All	All	All
Application	Cisco	Unified Service Monitor	8.0	All	All	All
Application	Cisco	Unified Service Monitor	All	All	All	All
Application	Emc	Ionix Acm	All	All	All	All
Application	Emc	Ionix Asam	All	All	All	All
Application	Emc	Ionix Ip	All	All	All	All

## References

Reference	Source	Link
Cisco Systems - Redirect to	CISCO	<a href="http://www.cisco.com">www.cisco.com</a>
Cisco Systems - Redirect to	CISCO	<a href="http://www.cisco.com">www.cisco.com</a>
Cisco Unified Service Monitor Flaw Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	<a href="http://www.securitytrac">www.securitytrac</a>
CiscoWorks LAN Management Solution Two Buffer Overflow Vulnerabilities - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</a>
EMC Ionix Products Service Two Buffer Overflow Vulnerabilities - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</a>
EMC Ionix Buffer Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	<a href="http://www.securitytrac">www.securitytrac</a>
Multiple EMC Ionix Applications Malformed Message Remote Buffer Overflow Vulnerability	BID	<a href="http://www.securityfoc">www.securityfoc</a>
75442	OSVDB	<a href="http://www.osvdb.org">www.osvdb.org</a>
IBM X-Force Exchange	XF	<a href="http://exchange.xforce">exchange.xforce</a>
Cisco Products Two Buffer Overflow Vulnerabilities - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Multiple Cisco Products CVE-2011-2738 Remote Code Execution Vulnerability	BID	<a href="http://www.securityfoc">www.securityfoc</a>
About Secunia Research   Flexera	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Cisco Unified Operations Manager Flaw Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	<a href="http://www.securitytrac">www.securitytrac</a>
CiscoWorks LAN Management Solution Flaw Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	<a href="http://www.securitytrac">www.securitytrac</a>
SecurityFocus	BUGTRAQ	<a href="http://www.securityfoc">www.securityfoc</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)