

Cisco Security Advisory: CiscoWorks Internetwork Performance Monitor CORBA GIOP Overflow Vulnerability

Advisory ID: cisco-sa-20100120-ipm

<http://www.cisco.com/warp/public/707/cisco-sa-20100120-ipm.shtml>

Revision 1.0

For Public Release 2010 January 20 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of this Notice: FINAL](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

Summary

CiscoWorks Internetwork Performance Monitor (IPM) versions 2.6 and earlier for Microsoft Windows operating systems contain a buffer overflow vulnerability that could allow a remote unauthenticated attacker to execute arbitrary code. There are no workarounds for this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20100120-ipm.shtml>.

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ Affected Products

☐ Vulnerable Products

CiscoWorks IPM versions 2.6 and earlier for Windows operating systems are affected.

☐ Products Confirmed Not Vulnerable

CiscoWorks IPM version 2.x for Sun Solaris and CiscoWorks IPM version 4.x for Windows and Solaris operating systems are not affected. No other Cisco products are currently known to be affected by this vulnerability.

[Top of the section](#) [Close Section](#)

☐ Details

CiscoWorks IPM is a troubleshooting application that gauges network response time and availability. CiscoWorks IPM is available as a component within the CiscoWorks LAN Management Solution (LMS) bundle. CiscoWorks IPM versions 2.6 and earlier for Windows contain a buffer overflow vulnerability when processing Common Object Request Broker Architecture (CORBA) GIOP requests. By sending a crafted CORBA GIOP request, a remote, unauthenticated attacker may be able to trigger the buffer overflow condition and execute arbitrary code with *SYSTEM* privileges on affected Windows systems. This vulnerability is documented in Cisco Bug ID CSCsv62350 and has been assigned the Common Vulnerabilities and Exposures (CVE) CVE-2010-0138.

☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at:

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at:

<http://intellishield.cisco.com/security/alertmanager/cvss>

CSCsv62350 - Malformed CORBA GIOP request causes crash (registered customers only)					
Calculate the environmental score of CSCsv62350					
CVSS Base Score - 10					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - 9.5					
Exploitability		Remediation Level		Report Confidence	
Functional		Unavailable		Confirmed	

☐ Impact

Successful exploitation of the vulnerability may result in the ability to execute arbitrary code with *SYSTEM* privileges on affected Windows systems.

[Top of the section](#) [Close Section](#)

☐ Software Versions and Fixes

Ciscoworks IPM versions 2.6 and earlier for Windows contain a vulnerable third-party component that is no longer supported. Cisco is unable to provide updated software for affected CiscoWorks versions. Consult the [Obtaining Fixed Software](#) section of this advisory for instructions on how to address vulnerable systems.

[Top of the section](#) [Close Section](#)

☐ Workarounds

There are no workarounds for this vulnerability. It is possible to mitigate this vulnerability by restricting network access to TCP ports on an affected Windows system running IPM versions 2.6 and earlier to trusted systems.

Additional mitigation techniques that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory:

<http://www.cisco.com/warp/public/707/cisco-amb-20100120-ipm.shtml>

[Top of the section](#) [Close Section](#)

☐ Obtaining Fixed Software

Ciscoworks IPM versions 2.6 and earlier for Windows contain a vulnerable third-party component that is no longer supported. Cisco is unable to provide updated software for affected CiscoWorks versions.

Customers with active software licenses for the IPM component of CiscoWorks versions 2.6 and earlier for Windows should send email to the following address for instructions on migrating to non-vulnerable software:

ipm-corba-fix@cisco.com

[Top of the section](#) [Close Section](#)

☐ **Exploitation and Public Announcements**

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

This vulnerability was discovered and reported to Cisco by an anonymous researcher working with TippingPoint's Zero Day Initiative. Cisco would like to thank TippingPoint for reporting this vulnerability to us and for working with us on a coordinated disclosure.

[Top of the section](#) [Close Section](#)

☐ **Status of this Notice: FINAL**

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

[Top of the section](#) [Close Section](#)

☐ **Distribution**

This advisory is posted on Cisco's worldwide website at:

<http://www.cisco.com/warp/public/707/cisco-sa-20100120-ipm.shtml>

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

[Top of the section](#) [Close Section](#)

☐ Revision History

Revision 1.0	2010-January-20	Initial public release
--------------	-----------------	------------------------

[Top of the section](#) [Close Section](#)

☐ Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

[Top of the section](#) [Close Section](#)

Help us help you.



Please rate this document.



Excellent

Good

Average

Fair

Poor



This document solved my problem.



Yes

No

Just browsing



Suggestions for improvement:

(256 character limit)



[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 - 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) |

[Trademarks of Cisco Systems, Inc.](#)