

# Cisco Security Advisory: Hardening of Solaris OS for MGC

Document ID: 20645

Advisory ID: cisco-sa-20020807-solaris-mgc

<http://www.cisco.com/warp/public/707/cisco-sa-20020807-solaris-mgc.shtml>

## Revision 1.0

Last Updated 2001 April 13 1700 UTC (GMT)

For Public Release 2002 August 07 1500 UTC (GMT)

---

Please provide your feedback on this document.

---

**Summary**  
**Affected Products**  
**Details**  
**Impact**  
**Software Versions and Fixes**  
**Workarounds**  
**Obtaining Fixed Software**  
**Exploitation and Public Announcements**  
**Status of This Notice: INTERIM**  
**Distribution**  
**Revision History**  
**Cisco Security Procedures**

---

## Summary

The Media Gateway Controller (MGC) product is installed on top of Solaris operating system. In the default installation Solaris has several know security vulnerabilities. In order to prevent them from being exploited customers must install updated packages CSCOh007 and CSCOh013. These packages contain the latest Solaris patches and additional hardening of the Solaris OS.

These vulnerabilities have been exploited and PSIRT knows of a few cases where customer's systems running SC2200 have been compromised.

We are investigating other products that are based on Solaris.

There is no workaround.

This advisory is available at the  
<http://www.cisco.com/warp/public/707/cisco-sa-20020807-solaris-mgc.shtml>.

## Affected Products

This section provides details on affected products.

## Vulnerable Products

The following products are affected:

SC2200	All systems running Solaris 2.6 (Through release 7.4(x))
VSC3000	All systems running Solaris 2.6 (Through release 9.1(x))
PGW 2200	All systems running Solaris 2.6 (Through release 9.1(x))
Billing and Management Server (BAMS)	All systems running Solaris 2.6
Voice Services Provisioning Tool (VSPT)	All systems running Solaris 2.6

We are investigating other Solaris based products.

## Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by these vulnerabilities.

## Details

The following issues are covered by this advisory:

- Installing the latest verified patches for the Solaris OS
- Securing the default Solaris OS installation
- Detecting the signs of a computer compromise

In order to guarantee the stability of the application Cisco must perform regression testing with all new patches installed. We evaluate every new Solaris patch and, depending on its severity on the overall system, new patches are provided either periodically or as soon as testing is finished.

Depending on the Solaris version Cisco provides a different patch bundle. Patches for Solaris 2.6 are provided in the package **CSCOh007.pkg**.

The second issue is the security of the default Solaris installation. By default, Solaris is installed with many services installed. Some of the services are known to have security issues. In order to minimize security exposure we strongly advise that you disable these services using the **CSCOh013.pkg** package.

The provided patches and the script will not help you if the computer was already compromised. In order to establish if your computer has been compromised or not consult the document at <http://www.cert.org/security-improvement/modules/m09.html>. If you are in doubt regarding this issue you may open a case with TAC and ask for further clarification of your results. The only way to guarantee that

your computer is not compromised is to reinstall Solaris and the application from the scratch.

## Impact

### Solaris patches

By not installing the latest Solaris patches the customer is exposed to various known vulnerabilities. By exploiting these vulnerabilities, customer's computer can be compromised, controlled, and used for unauthorized purposes.

### Disabling unneeded services

By leaving unneeded services running the customer is exposed to various security issues more than necessary. Running unneeded services also uses a small amount of CPU unnecessarily.

## Software Versions and Fixes

The issues are fixed with the following packages:

SC2200	All release up to and including 7.4(x)	MGCSOL-h007.bin and MGCSOL-h013.bin
VSC3000	All releases up to and including release 9.1(x)	MGCSOL-h007.bin and MGCSOL-h013.bin
PGW 2200	All releases up to and including release 9.1(x)	MGCSOL-h007.bin and MGCSOL-h013.bin
Billing and Management Server (BAMS)	All systems running Solaris 2.6	MGCSOL-h007.bin only
Voice Services Provisioning Tool (VSPT)	All systems running Solaris 2.6	MGCSOL-h007.bin only

To follow the software links below, you must be a registered user and you must be logged in.

Since vulnerabilities are in the underlying Operating System customers do not have to change or upgrade their application. The updated packages are MGCSOL-h007.bin (CSCOh007.pkg) and MGCSOL-h013.bin (CSCOh013.pkg). Their version is 1.0.7.

To follow the link below, you must be a registered user and you must be logged in.

Customers of the products listed above should check <http://www.cisco.com/cgi-bin/tablebuild.pl/mgc-sol> periodically for updates that apply to the Solaris OS used in the listed products. Instructions on the application of these Solaris packages are covered in the Cisco MGC Software Release (7 or 9) Installation & Configuration Guide. See the section entitled "Installing the Operating System Software."

To make these Solaris software packages easier to find, the information has also been linked to the Voice Software Center under each applicable software release of the Media Gateway Controller, BAMS and VSPT. This information can be located at <http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml>.

The Release Notes for the Solaris 2.6 packages are at <http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/relnote/sol26rn.htm>.

## Workarounds

There is no workaround. Although the user may perform all steps that are automated in packages CSCOh007.pkg and CSCOh013.pkg Cisco strongly discourages that. In order to guarantee the stability of the solution Cisco must perform regression testing. By removing a subsystem or installing a patch the customer may render the system unstable or inoperative.

## Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

## Customers with Service Contracts

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

## Customers using Third-party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

## Customers without Service Contracts

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are

as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: [tac@cisco.com](mailto:tac@cisco.com)

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

## Exploitation and Public Announcements

By exploiting some of known vulnerabilities in Solaris a few customers had their computers compromised. PSIRT has no evidence that these computers had been targeted because of the role they are playing. Intrudes seems to be oblivious of the computer's real purpose.

## Status of This Notice: INTERIM

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. CISCO EXPECTS TO UPDATE THIS DOCUMENT AS NEW INFORMATION BECOMES AVAILABLE.

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.

## Distribution

This notice will be posted on Cisco's Worldwide Web site at <http://www.cisco.com/warp/public/707/cisco-sa-20020807-solaris-mgc.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](mailto:cust-security-announce@cisco.com)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [comp.dcom.sys.cisco](mailto:comp.dcom.sys.cisco)
- [firewalls@lists.gnac.com](mailto:firewalls@lists.gnac.com)
- Various internal Cisco mailing lists

Future updates of this advisory, if any, will be placed on Cisco's Worldwide Web site, 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.

## Revision History

Revision 1.0	2002-Jan-16	Initial public release
--------------	-------------	------------------------

## 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 Web site at [http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](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>.

---

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Apr 13, 2001

Document ID: 20645

---