

# Cisco Security Advisory: Solaris /bin/login Vulnerability

Document ID: 22426

Advisory ID: cisco-sa-20020410-solaris-bin-login

<http://www.cisco.com/warp/public/707/cisco-sa-20020410-solaris-bin-login.shtml>

## Revision 1.0

For Public Release 2002 April 10 1600 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

This advisory describes a vulnerability that affects Cisco products and applications that are installed on the Solaris operating system, and is based on the vulnerability of a common service within the Solaris operating system, not due to a defect of the Cisco product or application. A vulnerability in the "/bin/login" program was discovered that enables an attacker to execute arbitrary code under Solaris OS. This vulnerability was discovered and publicly announced by Internet Security Systems Inc. All Cisco products and applications that are installed on Solaris OS are considered vulnerable to the underlying operating system vulnerability, unless steps have been taken to disable access services such as "bin/login."

We are investigating other Solaris-based products.

This vulnerability can be mitigated in many cases (not all), by limiting interactive logins to trusted hosts using access control list (ACL) or other mechanisms such as firewalls.

This advisory is available at the

<http://www.cisco.com/warp/public/707/cisco-sa-20020410-solaris-bin-login.shtml>.

## Affected Products

This section provides details on affected products.

## Vulnerable Products

All products and all releases that are running on top of Solaris OS are vulnerable because the vulnerability is within Solaris and not within the other applications.

The following products are affected:

### Media Gateway Controller (MGC) and Related Products

- Products running on Solaris 2.5.1 are vulnerable unless CSCOh008.pkg release 1.0(8) has been installed. The product that is based on this version of Solaris is Signaling Controller 2200 (SC2200).
- Products running on Solaris 2.6 are vulnerable unless CSCOh007.pkg release 1.0(7) has been installed. The products that are based on this version of Solaris are:
  - SC2200
  - Cisco Virtual Switch Controller (VSC3000)
  - Cisco PGW2200 Public Switched Telephone Network (PSTN) Gateway
  - Cisco Billing and Management Server (BAMS)
  - Cisco Voice Services Provisioning Tool (VSPT)

### Cisco IDS

- All releases of Cisco Secure Intrusion Detection System (IDS, formerly Netranger) up to, but excluding, 3.0(5)Sx, where "5" is the Service Pack and not the Signature Update field.

Other Cisco software applications may run on Solaris platforms and where those products have not specifically been identified, customers should install security patches regularly in accordance with their normal maintenance procedures.

We are investigating other Solaris-based products.

## Products Confirmed Not Vulnerable

PGW2200 release 9.2(2) running on Solaris 2.8 is not affected. The installation CD set contains the package CSCOh015, version 2.0.1, that includes the patch for this issue.

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

## Details

All implementations of the "login" program (also known as "/bin/login" due to its location on the file system) derived from the SysV implementation are vulnerable to a buffer overflow. This vulnerability can be exploited to gain unauthorized access to a computer system without possessing legitimate credentials. The only prerequisite for exploiting this vulnerability is to have Telnet or other remote login access to the computer because there are multiple ways to access a computer remotely. Telnet, rlogin, rsh, SSH, and X term are the most commonly known methods. This vulnerability can be exploited locally and remotely.

## Impact

By gaining unauthorized access an attacker can view and modify any part of the operating system possibly leading to a breach of confidentiality and integrity of the system.

# Software Versions and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") or your contracted maintenance provider for assistance.

## MGC and Related Products

- For the SC2200, the package CSCOh008.pkg release 1.0(8) contains the fix. The installation instruction is included within the package.
- For the products based on Solaris 2.6, the package CSCOh007.pkg release 1.0(7), or higher, contains the fix. The installation instruction is included within the package. This is applicable to the following products:
  - SC2200
  - VSC3000
  - PGW2200 PSTN Gateway
  - BAMS
  - VSPT

Both packages are available at <http://www.cisco.com/cgi-bin/tablebuild.pl/mgc-sol>.

For all MGC and related products, you may also consult "Cisco Security Advisory: Hardening of Solaris OS for MGC" located at <http://www.cisco.com/warp/public/707/Solaris-for-MGC-pub.shtml>.

## Cisco IDS

For IDS, release 3.0(5) is the first fixed release. The fixed software can be downloaded from <http://www.cisco.com/cgi-bin/tablebuild.pl/ids-appsens>.

## Workarounds

There is no workaround for MGC and related products.

For IDS, it is possible to mitigate the exposure by limiting hosts that can Telnet to IDS. This procedure is described at:

[http://www.cisco.com/en/US/docs/net\\_mgmt/cisco\\_info\\_center\\_for\\_security\\_monitoring/3.5/administration/guide/pre](http://www.cisco.com/en/US/docs/net_mgmt/cisco_info_center_for_security_monitoring/3.5/administration/guide/pre)

In short, the user must login to the IDS machine as root, type **sysconfig-sensor** at the prompt, select **option 5**, and enter the hosts allowed to Telnet to the sensor.

## 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

This vulnerability has been discovered by ISS Inc. and has been disclosed publicly. The advisories are published at:

- [http://www.iss.net/security\\_center/alerts/advise105.php](http://www.iss.net/security_center/alerts/advise105.php)
- <http://www.cert.org/advisories/CA-2001-34.html>

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

## 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 advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20020410-solaris-bin-login.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 notice, if any, will be placed on Cisco's worldwide web server, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the URL given above for any updates.

## Revision History

Revision 1.0	2002-April-10	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 website 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>.