

# Cisco Security Advisory: Cisco Security Advisory: Vulnerabilities in Cisco SN 5420 Storage Routers

Document ID: 13643

Advisory ID: cisco-sa-20010711-sn-kernel

<http://www.cisco.com/warp/public/707/cisco-sa-20010711-sn-kernel.shtml>

## Revision 1.0

For Public Release 2001 July 11 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: FINAL**  
**Distribution**  
**Revision History**  
**Cisco Security Procedures**

---

## Summary

Two vulnerabilities have been discovered in Cisco SN 5420 Storage Router software releases up to and including 1.1(3). One of the vulnerabilities can cause a Denial-of-Service attack. The other allows unrestricted low level access to the SN 5420.

There is no workaround for these vulnerabilities. It is possible to mitigate them by blocking access to ports 513 and 8023 on the network edge.

The vulnerabilities are documented in Cisco Bug IDs **CSCdu27529** and **CSCdu27514**.

No other Cisco product is affected by these vulnerabilities.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20010711-sn-kernel.shtml>.

## Affected Products

This section provides details on affected products.

## Vulnerable Products

Cisco SN 5420 Storage Routers running software release up to and including 1.1(3) are affected by the vulnerabilities.

To determine your software release, type **show system** at the command prompt.

## Products Confirmed Not Vulnerable

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

## Details

This section provides details about these vulnerabilities.

### CSCdu27529

You can reboot the device by rapidly establishing multiple connections to TCP port 8023.

### CSCdu27514

When logging into SN 5420 using "rlogin" or when connecting to the port 8023 from the GigabitEthernet or management interface, a user can access a developer's shell of the SN 5420. The user is not asked for a password. No other authorization is performed. This shell is used for testing during development.

Starting with software release 1.1(4), this capability is removed from the software.

## Impact

By repeatedly exploiting **CSCdu27529**, it is possible to prevent a user from accessing storage, thus causing a Denial-of-Service attack.

When logged into a developer's shell (**CSCdu27514**), users can execute debug commands, start and stop processes, and interfere with the normal process execution. Users who are logged in in such a manner and all commands executed by them are not logged or shown using the standard logging mechanism of the Cisco SN 5420 Storage Router.

## Software Versions and Fixes

The vulnerabilities are fixed in release 1.1(4) of the software, which is available on CCO.

## Workarounds

There is no workaround for these vulnerabilities. It is possible to mitigate them by blocking access to ports 513 and 8023 on the network edge.

## 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

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

in this advisory.

These vulnerabilities were found internally during product installation.

## 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.

## Distribution

This advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20010711-sn-kernel.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 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.

## Revision History

Revision 1.0	2001 July 11	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>.

---

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

---

