

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

Document ID: 17867

Advisory ID: cisco-sa-20020109-sn-vulnerabilities

<http://www.cisco.com/warp/public/707/cisco-sa-20020109-sn-vulnerabilities.s>

## Revision 1.0

For Public Release 2002 January 09 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: FINAL**  
**Distribution**  
**Revision History**  
**Cisco Security Procedures**

---

## Summary

Three vulnerabilities have been discovered in Cisco SN 5420 Storage Router software releases up to and including 1.1(5). Two of the vulnerabilities can cause a Denial-of-Service attack. The other allows access to the SN 5420 configuration if it has been previously saved on the router.

There is no workaround for these vulnerabilities.

No other Cisco product is vulnerable.

This advisory is available at  
<http://www.cisco.com/warp/public/707/cisco-sa-20020109-sn-vulnerabilities.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(5) are affected by the vulnerabilities. Please note that 1.1(6) version of the software was never released by Cisco.

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 this vulnerability.

- **CSCdv24925** — It is possible to read stored configuration files from the Storage Router without any authorization.
- **CSCdu32533** — By sending a HTTP request with huge headers, it is possible to crash the Storage Router.
- **CSCdu45417** — It is possible to halt the Storage Router by sending a fragmented packet over the Gigabit interface.

## Impact

Successful exploitation of the vulnerability may result in these issues:

- **CSCdv24925** — An unauthorized person may read the configuration of the Storage Router. This may lead to unauthorized access of a storage space.
- **CSCdu32533** — By exploiting this vulnerability, an attacker can cause Denial-of-Service.
- **CSCdu45417** — By exploiting this vulnerability, an attacker can cause Denial-of-Service.

## Software Versions and Fixes

All three vulnerabilities are fixed in release 1.1(7) of the software, which is available on CCO. Please note that version 1.1(6) of the software was never released by Cisco.

## Workarounds

This section describes workarounds for these vulnerabilities.

- **CSCdv24925** — It is possible to mitigate this vulnerability by blocking access on the network's edge and by using hard to guess names for saved configuration.
- **CSCdu32533** — There is no workaround for this vulnerability.
- **CSCdu45417** — There is no workaround for this vulnerability.

## 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 testing.

## 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-20020109-sn-vulnerabilities.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 | <del>2002-Jan-09</del> | <del>Initial public release.</del> |
|--------------|------------------------|------------------------------------|

## 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.

---

Updated: Jan 09, 2002

Document ID: 17867

---