

[NEWS] Multiple Vulnerabilities in Cisco SN 5420 Storage Routers

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0035.html>

From: support@securiteam.com

Date: 01/10/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 10 Jan 2002 10:13:51 +0100 (CET)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Multiple Vulnerabilities in Cisco SN 5420 Storage Routers

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 condition. The third allows access to the SN 5420 configuration if it has been previously saved on the router.

There is no workaround for these vulnerabilities.

DETAILS

Affected 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.

No other Cisco products are affected.

Securiteam: [NEWS] Multiple Vulnerabilities in Cisco SN 5420 Storage Routers

Details:

CSCdv24925

It is possible to read stored configuration file from the Storage Router without any authorization.

CSCdu32533

By sending an HTTP request with a large header, 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:

CSCdv24925

An unauthorized person may read the configuration of the Storage Router. That 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 the 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.

Obtaining Fixed Software

Cisco is offering free software upgrades to eliminate this vulnerability for all affected customers.

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 Web site at <<http://www.cisco.com>> <http://www.cisco.com>.

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 assistance with the upgrade, which should be free of charge.

Workarounds

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.

Securiteam: [NEWS] Multiple Vulnerabilities in Cisco SN 5420 Storage Routers

CSCdu45417

There is no workaround for this vulnerability.

ADDITIONAL INFORMATION

The information has been provided by <mailto:psirt@cisco.com> Cisco Systems Product Security Incident Response Team.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- *Previous message:* support@securiteam.com: "[NEWS] New Virus Infects Macromedia Flash Files"
 - *Messages sorted by:* [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)