

[NEWS] Vulnerabilities in Cisco SN 5420 Storage Routers

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-08/0057.html>

From: support@securiteam.com

Date: 08/11/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [NEWS] Vulnerabilities in Cisco SN 5420 Storage Routers

Message-Id: <20010811121622.7D766138BF@mail.der-keiler.de>

Date: Sat, 11 Aug 2001 14:16:22 +0200 (CEST)

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

Vulnerabilities in Cisco SN 5420 Storage Routers

SUMMARY

Two vulnerabilities have been discovered in Cisco SN 5420 Storage Router software release up to and including 1.1(3). One of the vulnerabilities can cause 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.

DETAILS

Affected 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.

No other Cisco products are affected by these vulnerabilities.

Securiteam: [NEWS] Vulnerabilities in Cisco SN 5420 Storage Rou

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 during developing for testing.

Starting with software releases 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 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 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 the release 1.1(4) of the software, which is available on CCO.

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>> <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:

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.

Exploitation and public announcements:

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

Securiteam: [NEWS] Vulnerabilities in Cisco SN 5420 Storage Rou

These vulnerabilities were found internally during product installation.

ADDITIONAL INFORMATION

The information has been provided by

<mailto:Cisco_Systems_Product_Security_Incident_Response_Team@exxonmobil.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: "[EXPL] Security Vulnerability found in /usr/bin/locate (Exploit Code)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)