

[NEWS] Cisco CatOS Embedded HTTP Server Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0064.html>

From: support@securiteam.com

Date: 10/16/02

From: support@securiteam.com

To: list@securiteam.com

Date: 16 Oct 2002 23:53:15 +0200

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.

Cisco CatOS Embedded HTTP Server Buffer Overflow

SUMMARY

Cisco Catalyst switches running specific versions of Cisco CatOS software are vulnerable to a buffer overflow in an embedded HTTP server. Only CatOS versions from 5.4 up to and including 7.3 which contain a "cv" in the image name are affected. If the HTTP server is enabled a buffer overflow can be remotely exploited which will cause the switch to fail and reload. The vulnerability can be exploited repeatedly and result in a denial of service.

Workarounds are available that limit the ability to exploit the vulnerability.

DETAILS

Affected Products:

This vulnerability is only present in Cisco Catalyst switches running Cisco CatOS software versions 5.4 through 7.3 that contain an embedded HTTP server to support CiscoView network management software. The affected software images contain "cv" in the image name as seen here: cat6000-supcv.5-5-16.bin.

Securiteam: [NEWS] Cisco CatOS Embedded HTTP Server Buffer Overflow

Details:

If the HTTP server is enabled on a Cisco Catalyst switch running an affected CiscoView image, an overly long HTTP query can be received by the embedded HTTP server that will cause a buffer overflow and result in a software reset of the switch. Once the switch has recovered and has resumed normal processing it is vulnerable again. It remains vulnerable until the HTTP server is disabled, HTTP queries to the switch management port are blocked, or the switch's software has been upgraded to a fixed version.

The HTTP server is disabled by default. It is typically enabled to allow web based management of the switch using CiscoView. Only a small subset of CatOS images contains this embedded HTTP server.

This vulnerability is documented as DDTS:

CSCdy26428 – CatOS crash with web server enabled in http_get_token.

Impact:

The exploitation of this issue can result in a software forced reset of this device. Repeated exploitation may lead to a denial of service until the workaround for this vulnerability has been implemented or a fixed version of software has been loaded onto the device.

Software Versions and Fixes:

All versions of CatOS software with the embedded HTTP server are vulnerable prior to the fixed versions listed below. Each row of the table describes a release train and the platforms or products for which it is intended. If a given release train is vulnerable, then the earliest possible releases that contain the fix and the anticipated date of availability for each are listed in the Rebuild, Interim, and Maintenance columns. A device running any release in the given train that is earlier than the release in a specific column (less than the earliest fixed release) is known to be vulnerable, and it should be upgraded at least to the indicated release or a later version (greater than the earliest fixed release label).

When selecting a release, keep in mind the following definitions:

Maintenance

Most heavily tested and highly recommended release of any label in a given row of the table.

Interim

Built at regular intervals between maintenance releases and receives less testing. Interims should be selected only if there is no other suitable release that addresses the vulnerability, and interim images should be upgraded to the next available maintenance release as soon as possible. Interim releases are not available via manufacturing, and usually they are not available for customer download from CCO without prior arrangement with the Cisco Technical Assistance Center (TAC).

Securiteam: [NEWS] Cisco CatOS Embedded HTTP Server Buffer Overflow

For a table listing all available patches and fixes see:

<http://www.cisco.com/warp/public/707/catos-http-overflow-vuln.shtml#Software>
<http://www.cisco.com/warp/public/707/catos-http-overflow-vuln.shtml#Software>

Obtaining Fixed Software:

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/kobayashi/sw-center/sw-lan.shtml>
<http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml>.

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 obtaining the free software upgrade(s).

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)
- * email: tac@cisco.com.

See <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>
<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.

Please 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.

Please do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

Workarounds:

The HTTP server can be disabled on the on the Cisco switch.

This example shows how to disable the HTTP server:

```
Console (enable) set ip http server disable
HTTP server disabled.
```

The default setting for the HTTP server is disabled.

You may also choose to block access to port 80 for your Cisco switch. This can be done with any device with traffic filtering capabilities.

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: "[NT] Denial of Service in Sabre Desktop Reservation Client for Windows"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)