

Cisco Security Advisory: Catalyst 5000 Series 802.1x Vulnerability

Document ID: 13617

Advisory ID: cisco-sa-20010413-cat5k-8021x

<http://www.cisco.com/warp/public/707/cisco-sa-20010413-cat5k-8021x.shtml>

Revision 1.0

Last Updated 2002 August 07 0800 UTC (GMT)

For Public Release 2001 April 13 1400 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

When an 802.1x frame is received by an affected Catalyst 5000 series switch on a STP blocked port it is forwarded in that VLAN instead of being dropped. This causes a performance impacting 802.1x frames network storm in that part of the network, which is made up of the affected Catalyst 5000 series switches. This network storm only subsides when the source of the 802.1x frames is removed or one of the workarounds in the workaround section is applied. This vulnerability can be exploited to produce a denial of service (DoS) attack.

This vulnerability is documented as Cisco bug id CSCdt62732.

This notice will be posted at <http://www.cisco.com/warp/public/707/cisco-sa-20010413-cat5k-8021x.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

Cisco Catalyst 5000 series switches based on any of the following EARL (Encoded Address Recognition Logic) hardware revisions:

- EARL 1
- EARL 1+
- EARL 1++

and running any of the following switch software revisions:

- 4.5 (11) or earlier
- 5.5 (6) or earlier
- 6.1 (2) or earlier

are affected by this vulnerability. This series includes the Catalyst models 5000, 5002, 5500, 5505, 5509, 2901, 2902 and 2926 switches.

To determine your hardware and software revision type **sh mod** on the console prompt of the switch.

Additional information can be found in the document, "Identifying Catalyst 5000 EARL Version and Other Common EARL Questions."

Products Confirmed Not Vulnerable

Catalyst 5000 series switches based on EARL 2 or later hardware revisions are not affected by this vulnerability.

Catalyst 5000 series switches regardless of the EARL hardware revision, running the following switch software revisions

- 4.5 (12) or later – expected general availability before 2001, May 1
- 5.5 (7) or later
- 6.1 (3) or later

are not affected by this vulnerability.

No other Cisco product is currently known to be affected by this vulnerability. This includes the Catalyst 6000, 4000, 3500XL, 2900XL and 2948G switches.

Details

When an 802.1x (IEEE standard for port based network access control) frame is received by an affected Catalyst 5000 series switch on a STP (Spanning Tree Protocol) blocked port it is forwarded in that VLAN (Virtual Local Area Network) instead of being dropped. This causes a performance impacting 802.1x frames network storm in that part of the network, which is made up of the affected Catalyst 5000 series switches. This network storm only subsides when the source of the 802.1x frames is removed or one of the workarounds in the workaround section is applied.

This vulnerability is documented as Cisco bug id CSCdt62732, which requires a CCO account to view.

Impact

When an affected Catalyst 5000 series switch network receives an 802.1x frame it causes an 802.1x frames network storm. This network storm degrades the performance of the network. Slower ports on the affected Catalyst 5000 series switches may stop passing user data. The affected Catalyst 5000 series switches may not respond to any management inquiries via SNMP, Telnet or HTTP. However, management via the console port on the switches is still possible and can be used to apply the workarounds.

Software Versions and Fixes

This vulnerability has been fixed in the following switch software revisions

- 4.5 (12) or later – expected availability before 2001, May 1
- 5.5 (7) or later
- 6.1 (3) or later

and the fix will be carried forward in all future releases.

Software upgrade can be performed via the console interface.

Workarounds

The following workarounds will prevent the 802.1x frames from causing an 802.1x frames network storm in an affected Catalyst 5000 series switch network.

These workarounds can also be applied to a network experiencing an 802.1x frames network storm.

1. Configure permanent MAC address entries for the entire reserved STP range 01-80-c2-00-00-02 to 01-80-c2-00-00-0f to be directed out an unused port for each VLAN on each affected switch in the network.

The commands to configure are given below.

```
set cam permanent 01-80-c2-00-00-02 <mod#>/<port#> <VLAN>
set cam permanent 01-80-c2-00-00-03 <mod#>/<port#> <VLAN>
set cam permanent 01-80-c2-00-00-04 <mod#>/<port#> <VLAN>
set cam permanent 01-80-c2-00-00-05 <mod#>/<port#> <VLAN>
set cam permanent 01-80-c2-00-00-06 <mod#>/<port#> <VLAN>
set cam permanent 01-80-c2-00-00-07 <mod#>/<port#> <VLAN>
set cam permanent 01-80-c2-00-00-08 <mod#>/<port#> <VLAN>
set cam permanent 01-80-c2-00-00-09 <mod#>/<port#> <VLAN>
set cam permanent 01-80-c2-00-00-0a <mod#>/<port#> <VLAN>
set cam permanent 01-80-c2-00-00-0b <mod#>/<port#> <VLAN>
set cam permanent 01-80-c2-00-00-0c <mod#>/<port#> <VLAN>
set cam permanent 01-80-c2-00-00-0d <mod#>/<port#> <VLAN>
set cam permanent 01-80-c2-00-00-0e <mod#>/<port#> <VLAN>
set cam permanent 01-80-c2-00-00-0f <mod#>/<port#> <VLAN>
```

2. Break the STP loop by either
 - a. Disabling the redundant (STP blocked ports) or
 - b. Disconnecting the cable from these portsRemove all the sources of 802.1x frames before re-enabling the ports or reconnecting the cables.
3. Power down the Catalyst 5000 switch(es) that create the spanning-tree loop (any switch with STP blocked ports).
Remove all the sources of 802.1x frames before powering up the switches.

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

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 malicious use of the vulnerability described in this advisory.

A customer who discovered this vulnerability while using Microsoft Windows XP BETA software reported this vulnerability to Cisco. Microsoft Windows XP attempts 802.1x authentication during its boot-up phase. Following these configuration steps can disable this:

1. Click on the associated Local Area Connection under Network Connections
2. Click on the Authentication Tab at the top right.
3. Uncheck "Network Access Control using IEEE 802.1x"

This issue has been discussed in news articles regarding issues with Microsoft Windows XP BETA program and the Cisco Catalyst 5000 series switches.

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-20010413-cat5k-8021x.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
- bugtraq@securityfocus.com
- firewalls@lists.gnac.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- comp.dcom.sys.cisco
- 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 1.1	2002-August-07	
--------------	----------------	--

Revision 1.0	2001–April–13	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. 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: Apr 13, 2001

Document ID: 13617
