

# Cisco Security Advisory: TCP Loopback DoS Attack (land.c) and Cisco Devices

Document ID: 13661

Advisory ID: cisco-sa-19971121-land

<http://www.cisco.com/warp/public/707/cisco-sa-19971121-land.shtml>

## Revision 6.0

Last Updated 1997 December 11 0100 UTC (GMT)

For Public Release 1997 November 21 2200 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: INTERIM](#)  
[Distribution](#)  
[Revision History](#)  
[Cisco Security Procedures](#)

---

## Summary

Somebody has released a program, known as **land.c**, which can be used to launch denial of service attacks against various TCP implementations. The program sends a TCP SYN packet (a connection initiation), giving the target host's address as both source and destination, and using the same port on the target host as both source and destination.

- **Classic Cisco IOS software** (used on Cisco routers with product numbers greater than 1000, on the CGS/MGS/AGS+, on the CS-500, and, in a variant form, on the Lightstream 1010 ATM switch) has been verified to be vulnerable to this attack, depending on the software version. See the Software Versions and Fixes section of this document for information on affected versions.
- **Cisco IOS/700 software** (used on Cisco 7xx routers) has also been verified to be vulnerable.
- **Catalyst 5xxx and 29xx LAN switches** are vulnerable to the attack. Failures to reproduce the failure in early Cisco lab testing were caused by errors introduced by the kernels on the machines being used to run the attack program. Other Catalyst switches do not share any TCP code with the Catalyst 5xxx or 29xx, and have shown no vulnerability in any tests.
- Cisco **BPX and IGX WAN switches** are vulnerable under some circumstances. These switches can be attacked *only* via their management ports, not from the transit data stream.

- The **AXIS shelf** is affected by the attack. The AXIS shelf can be attacked only via its management port.
- The **PIX firewall** has been tested, and does **not** appear to be affected.
- The **Centri firewall** has been tested, and does **not** appear to be affected.

This advisory will be posted at: <http://www.cisco.com/warp/public/707/cisco-sa-19971121-land.shtml>.

## Affected Products

### Vulnerable Products

All Cisco IOS/700 software systems that can be reached via TCP from untrusted hosts are affected. Classic Cisco IOS software systems that are running vulnerable versions and that can be reached via TCP from untrusted hosts are affected. All Cisco Catalyst 5xxx and 29xx switches that can be reached via TCP from untrusted hosts are affected. IGX and BPX WAN switches, and the AXIS shelf, are affected, but only if their management ports are exposed to the hostile packets.

In all cases, the TCP ports reachable by the attack must be ports on which services are actually being provided (such as the Telnet port, for most systems). The attack requires spoofing the target's own address, so systems behind effective anti-spoofing firewalls are safe.

### Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by these vulnerabilities.

## Details

This section provides details about these vulnerabilities.

### Classic Cisco IOS Software Details

Classic Cisco IOS software versions vary in their susceptibility to the land.c attack. Releases fall into highly vulnerable, moderately vulnerable, and largely invulnerable classes. Newer releases are less vulnerable than older releases.

#### Cisco IOS/700 Software

All Cisco IOS/700 software versions which have been evaluated are vulnerable to this attack. A Cisco IOS/700 system subjected to this attack will hang and must be physically reset.

#### Cisco Catalyst 5xxx and 29xx LAN Switch

Cisco Catalyst 5xxx and Catalyst 29xx LAN switches are vulnerable to attack. Both switch types crash when attacked. The crash may be preceded by a system hang of as much as a few seconds, but no systems have been observed to hang indefinitely. Bug ID CSCdj62723 has been assigned to this problem.

Other Catalyst LAN switches have been tested, and have not shown any vulnerability to the attack. Only the 5xxx and 29xx series are affected.

# Impact

This vulnerability allows attackers to deny service to legitimate users and to administrators. Recovery may require physically visiting the affected hardware. Appropriate firewalls and some configuration workarounds can block this attack.

This section describes only impacts. See the appropriate product-specific "Details" sections later in this document for information on software fixes and configuration workarounds.

## Classic Cisco IOS Software

Classic Cisco IOS software versions fall into three groups in terms of vulnerability.

- Highly vulnerable releases may hang indefinitely, requiring hardware resets, when attacked.
- Moderately vulnerable releases will not accept any new TCP connections for about 30 seconds after receiving an attack packet, permitting denial of service to administrators and possibly to users, but will recover and will continue to forward packets.
- Largely invulnerable releases will continue to operate normally with negligible performance impact.

See the Software Versions and Fixes section of this document for information on exactly which versions are affected.

## Cisco IOS/700 Software and 7xx Systems

Cisco 7xx systems subjected to the attack will hang indefinitely and must be physically reset.

## Cisco Catalyst 5xxx and 29xx LAN Switches

The Catalyst 5xxx and Catalyst 29xx switches are vulnerable to the attack. A Catalyst 5xxx or Catalyst 29xx subjected to the attack will hang for a few seconds, then reboot itself. No special circumstances appear to be required to make a switch vulnerable to the attack; any switch that can be reached via TCP is vulnerable.

There are no lasting ill effects, but the reboot process will disrupt network traffic for as much as a few minutes. Furthermore, the rebooted system is immediately vulnerable to renewed attack.

The original version of this notice said, based on a report from a customer, that Catalyst 5xxx LAN switches were vulnerable to this attack. A later notice said that Cisco had been unable to reproduce the problem. This turns out to have been because of an error in Cisco's internal testing; the systems being used to generate the attack packets were damaging the TCP header checksums and making the packets harmless. Thus, the initial version of the notice was correct, and the later "corrected" version was wrong.

## Cisco WAN-BU Products

The attack affects BPX and IGX WAN switches, but only when they are attacked via their Ethernet management ports. Other circumstances necessary to make the attack succeed have not been characterized. The impact observed has been in the form of hanging Telnet sessions and inability to create new sessions. It is unclear at this time whether or not the traffic forwarding functions of the switches are affected, or whether non-Telnet switch management functions are affected.

The attack causes minutes-long management service interruptions on the AXIS shelf. New TCP connections are not accepted, and old connections are not serviced. The tests that provided this information were done with minimal access to the AXIS shelf being tested, and further information about the impact is not available

at this time; it is possible that the AXIS shelf supervisory processor crashed and rebooted in response to the attack. Attacks on the AXIS shelf succeeded only when delivered via the management port. Other conditions required for the attack to succeed are not known at this time. Cisco will release a fix for this problem if it proves appropriate.

## Other Cisco Products

Tests indicate that the PIX firewall is not vulnerable to this attack. Tests have been conducted with versions 4.1.3.245 and 4.0.7.

Tests indicate that the Centri firewall (build 4.110) is not vulnerable to this attack, either with or without exposed services configured.

Tests indicate that Catalyst LAN switches other than the 5xxx and 29xx series are not vulnerable to this attack.

## Software Versions and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") or your contracted maintenance provider for assistance.

## Cisco IOS Software

### Affected Versions

There are two bugs that make Cisco IOS software vulnerable to this attack. Fixes exist in the field for both bugs. Bug ID CSCdi71085 makes systems highly vulnerable to the attack. Bug ID CSCdi87533 makes systems moderately vulnerable. Bug ID CSCdj61324 is a newly-created bug ID that is being used as a tag for integration of the fix for CSCdi87533, plus a largely cosmetic change that prevents even the temporary creation of a half-open connection. The fix for CSCdj61324 has not yet been integrated into any released code, but is not necessary if the fix for CSCdi87533 is present.

CSCdi71085 and CSCdj87533 divide Cisco IOS software versions into three vulnerability classes. Versions that do not have the fix for bug ID CSCdi71085 are highly vulnerable, and may hang indefinitely, requiring hardware resets, when attacked. This includes all releases before release 10.3, as well as early 10.3, 11.0, 11.1, and 11.2 versions. CSCdi71085 was fixed in 11.2(2), 11.2(2)P, and 11.2(2)F, as well as in the 10.3, 11.0, and 11.1 releases listed in the table below.

Versions in which CSCdi71085 has been fixed, but in which CSCdi87533 is still present, are moderately vulnerable to the attack. These versions will not accept any new TCP connections for about 30 seconds after any attack packet is received, but will not hang completely, will continue to forward packets without interruption, and will recover with no long-term effects. CSCdi87533 has thus far been fixed only in 11.2-based releases; the fix was integrated in 11.2(3.4), 11.2(3.4)F, and 11.2(3.4)P.

Versions in which both CSCdi71085 and CSCdi87533 have been fixed are largely invulnerable to this attack. These versions will create half-open TCP connections upon receiving attack packets, but will continue to

accept legitimate TCP connections, and will delete the half-open connections within about 30 seconds. The performance impact of such a half-open connection during its lifetime is believed to be negligible.

Future versions in which CSCdj61324 has been fixed will be invulnerable to the attack, and will not create half-open connections in response to attack packets. We believe the security advantage of the CSCdj61324 fix over the CSCdj87533 fix to be negligible; CSCdj61324 is largely a placeholder to be used for integrating fixes in future non-11.2 releases.

If you believe that there is any possibility of hostile attack against your system, and if you cannot protect yourself using the configuration workaround given above, we strongly recommend that you update your software to a version containing the fix for CSCdi71085, since the impact of CSCdi71085 under this attack is very high. The fix for CSCdi71085 is available for releases based on 10.3, 11.0, 11.1, and 11.2, and has been in the field for quite some time. Users of 11.2-based releases should install post-11.2(4) versions, thereby getting the fix for CSCdi87533 as well.

At the time of this writing, the following releases are recommended:

Base Release	First released versions with all existing fixes (*= fix for CSCdi87533)	Recommended for most installations
10.3	10.3(16)	10.3(19a)
11.0	11.0(12), 11.0(12a)BT	11.0(17), 11.0(17)BT
11.1	11.1(7), 11.1(7)AA, 11.1(7)CA, 11.1(9)IA	11.1(15), 11.1(15)AA, 11.1(15)CA, 11.1(15)IA
11.2	11.2(4)*, 11.2(4)F*, 11.2	11.2(10), 11.2(9)P, 11.2(4)F1
Before 10.3	End of engineering	10.3(19a)

As with any software update, you should make sure your system configuration is supported by the new software before installing it. It's especially important to make sure that your system has sufficient memory to support the new software. Update planning assistance is available from Cisco's Worldwide Web site at <http://www.cisco.com/>.

### Planned Fixes

Cisco intends to release fixes for CSCdj61324 (equivalent to CSCdi87533) on non-11.2 releases. Because the impact of CSCdj61324/CSCdi87533 is moderate, and because a configuration workaround exists, we do not intend to create special software releases for these fixes. The fixes will appear in regularly scheduled maintenance releases of 11.0 and 11.1 software. For more information on the workaround for this issue, see the Workarounds section of this document.

Release 10.3 is at end of engineering, and will not be fixed. Customers who absolutely must run 10.3 or older code, and who absolutely cannot install the workarounds described below, and who believe they are likely to be subject to attack, should contact the Cisco TAC.

The fixed code for 11.0 and 11.1 has been written and subjected to unit testing, and is now being scheduled for integration in future maintenance releases. These fixes are being treated as priority items.

## Cisco IOS/700 Software

Cisco plans to release a software fix for IOS/700. The fix code has been written, and is being tested for integration and release. Because there is a low-impact configuration workaround that provides complete protection against the attack, Cisco does not plan to expedite release of this software fix. The fix will appear in regularly scheduled IOS/700 maintenance releases.

## Catalyst 5xxx and 29xx LAN Switch

A software fix has been developed for the Catalyst 5xxx and 29xx switch software. Because the impact of land.c attack on these switches is severe, and because the available configuration workarounds are not practical for many customers, Cisco has produced interim software builds incorporating these fixes. Two interim versions are available: 2.1(1102) and 2.4(401).

Interim versions receive less testing than regular software releases, and Cisco's support resources for interim versions are more limited than support resources for regular releases. We ask that customers install these releases only if they believe their networks are at genuine risk of disruptive attack. Customers may obtain the interim software by contacting the Cisco TAC at +1 800 553 24HR.

The fix will be incorporated in the next regularly scheduled maintenance releases of both 2.1 and 2.4 Catalyst 5xxx and 29xx software.

## Workarounds

This section provides workarounds for these vulnerabilities.

### Cisco IOS Software

Classic Cisco IOS software users can use input access lists on their interfaces to prevent the attack packets from entering their TCP stacks. Input access lists are available in all Cisco IOS software versions from 9.21 onward. Using an input access list will prevent the attack entirely, but may have unacceptable performance impacts on heavily loaded high-end routers. Traffic will still be fast-switched, but higher-speed switching modes may be disabled by the use of the input access lists. Use care in deploying this workaround on heavily loaded routers.

If you have no existing input access lists, create a new IP extended access list. Use a presently-unused number between 100 and 199. The access list must have an entry for each IP address configured on the system. Deny packets from each address to itself. For example:

```
access-list 101 deny tcp 1.2.3.4 0.0.0.0 1.2.3.4 0.0.0.0
access-list 101 deny tcp 5.6.7.8 0.0.0.0 5.6.7.8 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

If you have existing access lists, you'll need to merge the new entries in an appropriate way, generally at the top of the list.

Once created, the access list should be applied incoming on all interfaces, so a fragment of a total router configuration might look like this:

```
interface ethernet 0
ip address 1.2.3.4 255.255.255.0
ip access-group 101 in
```

```
!  
interface ethernet 1  
ip address 5.6.7.8  
ip access-group 101 in  
!  
access-list 101 deny tcp 1.2.3.4 0.0.0.0 1.2.3.4 0.0.0.0  
access-list 101 deny tcp 5.6.7.8 0.0.0.0 5.6.7.8 0.0.0.0  
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

Cisco recommends that you take advantage of the opportunity provided by installing this workaround to review your anti-spoofing filters, if appropriate.

## Cisco IOS/700 Software

Add the following configuration command to any profile that may be active when connected to a potentially hostile network:

```
set ip filter tcp in source <7xx IP address> destination <7xx IP address> block
```

This will completely protect the 7xx system. We believe that 7xx configurations in which this command has unacceptable performance or other impact are extremely rare if they exist at all.

## Catalyst 5xxx and 29xx LAN Switch

The attack may be absolutely avoided by not assigning an IP address to the Catalyst switch. However, this has the effect of disabling all remote management. Depending on its location in the network, it may be possible to protect the switch with router access lists or dedicated firewalls. An example of an appropriate Cisco router access list entry for specifically protecting an individual switch would be:

```
access-list 101 deny ip <switch-address> 0.0.0.0 <switch-address> 0.0.0.0
```

Note that this single entry is not a complete access list, and should not be used without combining it with other entries that permit desired traffic. Other, more general filters are feasible.

## Using Cisco Products to Protect Other Systems

We do not believe that this attack can be used against systems behind our dedicated firewall products, the PIX and Centri firewalls, unless general-purpose tunnels have been enabled through the firewalls. Such configurations are not recommended.

Properly designed anti-spoofing access lists at border routers can be used to prevent the attack from entering a private network from the Internet. Use the access lists to filter out packets whose IP source addresses are on your internal net, but which are arriving from interfaces connected to the outside Internet. Such filters are strongly recommended not only because of this attack, but because of other known attacks which affect various network devices, and because new IP spoofing attacks are constantly surfacing. If at all possible, it's also desirable to configure access lists to prevent packets from being sent from your internal net to the Internet with source addresses that aren't actually part of your internal net. This can help to keep your network from being used as a launchpad for denial of service attacks.

## 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

Cisco has had multiple reports of this vulnerability.

Most exploitation seems to be using the original program, which sends one packet at a time. A similar

Cisco Security Advisory: TCP Loopback DoS Attack (land.c) and Cisco Devices

program, latierra.c, which is capable of flooding and of scanning port and address ranges, has been released, and it is reasonable to expect some flooding attacks.

This issue has been widely discussed in a variety of Internet forums. Exploitation code is widely available to the public.

Cisco first heard of this problem on the morning of Friday, November 21.

## Status of This Notice: INTERIM

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. CISCO EXPECTS TO UPDATE THIS DOCUMENT AS NEW INFORMATION BECOMES AVAILABLE.

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

Earlier versions of this notice were sent to, or announced in, the following Internet mailing lists and newsgroups:

- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [comp.dcom.sys.cisco](mailto:comp.dcom.sys.cisco)
- [bugtraq@netspace.org](mailto:bugtraq@netspace.org)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [nanog@merit.edu](mailto:nanog@merit.edu)

The existence of this version is being announced in those forums, but the full text is not being sent. Further updates will be announced as appropriate, but may not be announced in all the forums used up to now. If you have a special interest in this information, please check the Web version periodically.

This notice will be posted in the "Field Notices" section of Cisco's Worldwide Web site, which can be found under "Technical Tips" in the "Service and Support" section. The URL is:

<http://www.cisco.com/warp/public/707/cisco-sa-19971121-land.shtml>

The copy on the Worldwide Web will be updated as appropriate.

## Revision History

Revision 6.0	1997-DEC-10	Catalyst 5000 fix information. More detailed information about other fixes. General reformatting.
Revision 5.0	1997-NOV-28	Editing and typographical error correction

Revision 4.0	1997–NOV–28	The Catalyst 5000 <i>is</i> vulnerable; so is the 2900. Failures to reproduce the problem in house were caused by errors in the test setup. Other Catalyst switches were tested using the same setup, and may be vulnerable.
Revision 3.0	1997–NOV–26	Retract the claim that the Catalyst 5000 is vulnerable. Add information about IGX and BPX WAN switches and about the AXIS shelf.
Revision 2.0	1997–NOV–22	Add information about highly vulnerable Cisco IOS versions.  Add detailed information about affected version numbers.  Add specific bug IDs.  Add upgrade recommendations.  Add first information about Catalyst LAN switches.  General editing and reformatting.
Revision 1.0	1997–NOV–21	Initial revision

## Cisco Security Procedures

Please report security issues with Cisco products, and/or sensitive security intrusion emergencies involving Cisco products, to [security-alert@cisco.com](mailto:security-alert@cisco.com). Reports may be encrypted using PGP; public RSA and DSS keys for [security-alert@cisco.com](mailto:security-alert@cisco.com) are on the public PGP keyservers.

The alias [security-alert@cisco.com](mailto:security-alert@cisco.com) is used only for reports incoming to Cisco. Mail sent to [security-alert@cisco.com](mailto:security-alert@cisco.com) goes only to a very small group of users within Cisco. Neither outside users nor unauthorized Cisco employees may subscribe to [security-alert@cisco.com](mailto:security-alert@cisco.com). We will shortly be creating a security announcement mailing list for outgoing information. When that list is created, an announcement will be sent to appropriate Internet forums.

Please do not use [security-alert@cisco.com](mailto:security-alert@cisco.com) for configuration questions, for security intrusions that you do not consider to be sensitive emergencies, or for general, non–security–related support requests. We do not have the capacity to handle such requests through this channel, and will have to refer them to Cisco Technical Assistance Center, delaying response to your questions. We advise contacting the Technical Assistance Center directly with this type of question.

---

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jun 14, 2007

Document ID: 13661

Cisco Security Advisory: TCP Loopback DoS Attack (land.c) and Cisco Devices

