

# Cisco Security Advisory: Vulnerability in the zlib Compression Library

Document ID: 22266

Advisory ID: cisco-sa-20020403-zlib-double-free

<http://www.cisco.com/warp/public/707/cisco-sa-20020403-zlib-double-free.shtml>

## Revision 1.0

Last Updated 2002 May 22 2100 UTC (GMT)

For Public Release 2002 April 03 1600 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

There is a vulnerability in the zlib compression library. This code is used in multiple applications. While we have not identified any Cisco product that is directly impacted by the vulnerability, there are several products that are using third-party modules that are vulnerable or that are running on an operating system that is vulnerable. This vulnerability has been publicly disclosed.

Cisco PSIRT is still evaluating which products are affected by this vulnerability.

There is no workaround for this vulnerability.

This advisory is available at  
<http://www.cisco.com/warp/public/707/cisco-sa-20020403-zlib-double-free.shtml>.

## Affected Products

This section provides details on affected products.

# Vulnerable Products

The following products are affected:

## Cache Software/ACNS

- Content Engine 507, 560, 590, and 7320 running Cache Software 3.1.1 or Application and Content Networking Software 4.0.x or 4.1.1
- Content Router 4430 and Content Distribution Manager 4630 and 4650 running Application and Content Networking Software 4.0.x or 4.1.1

## ME1100

This product reached the end-of-life state in 2001. This product is no longer supported, and customers are strongly advised to migrate to a recent product.

## Cisco Intrusion Detection System

Cisco IDS sensor appliances (part numbers IDS-4210, IDS-4220-E and IDS-4230-xx) are vulnerable if the sensor version as reported by nrvrs is in the range 3.0(1) through 3.0(5) inclusive. The C6000 IDSM (part number WS-X6381-IDS) is not vulnerable.

## Metro 1500 DWDM

All releases prior to software release 3.3b are affected.

## Hosting Solution Engine (HSE)

HSE releases 1.0 and 1.3 are vulnerable.

We are still evaluating the rest of Cisco products against this vulnerability.

We have verified that the following products are not vulnerable or that exposure is negligible. Note that this is not an exhaustive list.

- Cisco IOS®
- Cisco CatOS
- Cisco SN 5420 Storage Routers
- PIX Firewall
- VPN 3000, 3500
- User Registration Tool (URT)

Some products, such as Cisco IOS, use compressed images. In order to utilize this attack vector, an attacker would have to prepare a tampered distribution image and try to load it onto a device. That implies either physical or administrative access to the device. By having such access, an attacker is in a position to execute many other attacks, some of which are much easier to accomplish. Although Cisco will incorporate the fixed version of zlib in the subsequent software releases for products that belong to this category, that fact will not be reflected in this advisory.

## Products Confirmed Not Vulnerable

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

## Details

There is a bug in the decompression algorithm used by the popular zlib compression library. By sending a crafted block of invalid compressed data, an attacker can cause the application to corrupt internal data. This happens when the application tries to uncompress the data.

In most cases this vulnerability will cause denial of service. However, depending on the right circumstances and applications, there is a potential that an attacker could execute an arbitrary code. This code would then be executed using the privileges of the application in question.

## Impact

By repeatedly exploiting this vulnerability, an attacker can cause denial of service. It is possible that an attacker may be able to execute an arbitrary code on the target machine. In that case, this may lead to a partial or total compromise of the machine in question.

## 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.

### Cache Software/ACNS

ACNS 4.1.3 is the fixed release. It will be available in the second half of April 2002.

### ME1100

This product has reached the end-of-life state and the fix is not scheduled. Customers are strongly advised to migrate to a recent product.

### Cisco Intrusion Detection System

Sensor appliance software version 3.1(2)S23 is the first fixed release. It is available from May 17, 2002.

### Metro 1500 DWDM

The software release 3.3b is the first fixed release. It will be available on April 5, 2002.

### Hosting Solution Engine

HSE release 1.4 contains the fix. It will be available on April 15, 2002.

Cisco Security Advisory: Vulnerability in the zlib Compression Library

## Workarounds

There is no workaround for this vulnerability.

## 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

This vulnerability was publicly announced by third parties on March 21, 2002. The related advisories can be found at:

- <http://www.cert.org/advisories/CA-2002-07.html>
- <http://www.gzip.org/zlib/advisory-2002-03-11.txt>

## 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

This advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20020403-zlib-double-free.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](mailto:cust-security-announce@cisco.com)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [comp.dcom.sys.cisco](mailto:comp.dcom.sys.cisco)
- [firewalls@lists.gnac.com](mailto:firewalls@lists.gnac.com)
- 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-May-22	Modified Software Versions and Fixes section
Revision	2002-April-03	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](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: May 22, 2002

Document ID: 22266

---