

Cisco Security Advisory



Advisory ID: cisco-sa-20010720-code-red-worm
Published: 2001 July 20 12:00 GMT
Version 2.3: Final
Workarounds: [See below](#)

[Download CVRF](#)

[Download PDF](#)

[Email](#)

Summary

A malicious self-replicating program known as the "Code Red" worm is targeted at systems running the Microsoft Internet Information Server (IIS). Several Cisco products are installed or provided on targeted systems. Additionally, the behavior of the worm can cause problems for other network devices.

The following Cisco products are vulnerable because they run affected versions of Microsoft IIS:

- Cisco CallManager
- Cisco Unity Server
- Cisco uOne
- Cisco ICS7750
- Cisco Building Broadband Service Manager
- IP/VC 3540 Application Server

Other Cisco products may also be adversely affected by the "Code Red" worm. Please see the [Affected Products](#) section for further details.

The worm and its effects may be remedied by applying the Microsoft patch to affected servers:

<http://www.microsoft.com/technet/security/Bulletin/MS01-033.msp>

This advisory is available at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010720-code-red-worm>

Affected Products

This section provides details on affected products.

Vulnerable Products

The following Cisco products are directly vulnerable because they run affected versions of Microsoft IIS:

- Cisco CallManager
- Cisco Unity Server
- Cisco uOne
- Cisco ICS7750
- Cisco Building Broadband Service Manager
- IP/VC 3540 Application Server

The following Cisco products may be vulnerable due to side-effects caused by the "Code Red" worm. They are not directly vulnerable to the Microsoft IIS exploit:

- Cisco IP/VC 3510 H.323 Videoconference Multipoint Control Units
- Cisco Aironet Wireless products
- Cisco CSS 11000 series Content Service Switches
- Cisco 600 Series of DSL routers that have not been patched for a previously published vulnerability
- Cisco IP Phone 7960, 7940, 7910
- CiscoSecure User Changeable Password software
- Cisco WebView

The following Cisco products may be installed on various web servers and are vulnerable if installed on a Microsoft IIS server:

- Cisco Collaboration Server (CCS)
- Cisco Dynamic Content Adapter (DCA)
- Cisco Media Blender (CMB)
- TrailHead (Part of the Web Gateway solution)

Various Cisco Network Management products may be installed on Microsoft platforms that may be running a vulnerable version of IIS. Much older versions of CiscoWorks 2000 RWAN/CWSI Campus v2.x and Cisco Voice Manager v1.x are directly vulnerable because IIS was required as a part of the installation. Such systems might be offering HTTP services on default ports. These specific software packages are no longer supported, but are included in this notice to alert customers that might still be using them.

Products Confirmed Not Vulnerable

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

Details

At least three versions of the "Code Red" worm are known to exist.

Both versions exploit a known vulnerability in Microsoft IIS by passing a specially crafted Uniform Resource Identifier (URI) to the default HTTP service, port 80, on a susceptible system. The URI in version 1 consists of binary instructions which cause the infected host to either begin scanning other random IP addresses and pass the infection on to any other vulnerable systems it finds, or launch a denial of service attack targeted at the IP address 198.137.240.91 which, until very recently, was assigned to www.whitehouse.gov . In both cases, the worm replaces the web server's default web page with a defaced page at the time of initial infection. Version 2 has the same behavior, except that it does not deface the default web page, and it no longer contains a hard-coded address for www.whitehouse.gov , opting instead to look up the address via DNS.

Version 1 does not produce a truly random list of addresses to attack, whereas version 2 contains a fixed randomizer that will attempt all possible IP addresses except those beginning with 127.x.x.x or 224.x.x.x. The worm does not check for pre-existing infection, so that any given system may be executing as many copies of the worm as have scanned it, with a compounding effect on system and network demand.

A newer variant named Code Red II is known to exploit the same vulnerability as the other Code Red strains, however the effects and damage to the local webserver are different. For more details, refer to the analysis of the worm at the following location:

<http://www.eeye.com/html/Research/Papers/DS20010802.html>

Cisco products that are directly vulnerable because they use IIS can be protected from infection by applying the recommended patches from Microsoft. Workarounds are available as a temporary measure.

Side-effects caused by the worm can expose unrelated problems on other products. When the traffic from the worm reaches a significant level, a Cisco CSS 11000 series Content Service Switch may suffer a memory allocation error that leads to memory corruption and will require a reboot. The defect is documented in DDTS CSCdu76237. Traffic from the worm can trigger a defect in the IP/VC 3510 Videoconference Multipoint Control Unit which is documented in DDTS CSCdv01788. Traffic from the worm can trigger a defect in the Cisco Aironet Wireless devices, which is documented in DDTS CSCdv01662.

As a separate side-effect, the URI used by the worm to infect other hosts causes Cisco 600 series DSL routers to stop forwarding traffic. An affected 600 series router that has been scanned by the "Code Red" worm may not resume normal service until the power has been cycled.

The nature of the "Code Red" worm's scan of random IP addresses and the resulting sharp increase in network traffic can noticeably affect Cisco routers running Cisco IOS software, depending on the device, its current configuration, and the topology of the network. Unusually high CPU utilization and memory starvation may occur, and it can be mitigated in many cases simply by refining the configuration. Troubleshooting and configuration recommendations are available at this location: http://www.cisco.com/warp/public/63/ts_codred_worm.shtml

Workarounds

We recommend following the instructions in the Microsoft security bulletin for addressing the actual vulnerability in IIS.

Workaround for CSS11000 Series Products

The memory allocation problem on the CSS 11000 Content Service Switches can be worked around by restricting XML access as shown:

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the [Security Vulnerability Policy](#). This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Subscribe to Cisco Security Notifications

[Subscribe](#)

```
configure
restrict xml
```

Workaround for Cisco 600 Series Products

To disable web management on port 80, set the web management port to some number greater than 1024, and configure the web remote address for a non-routeable address.

```
set web port number_greater-than_1024
set web remote 10.10.10.10
```

Workaround for Cisco Aironet Wireless Bridge or Access Point: Disable Web Management

For the AP4800 series and Aironet Bridge devices, from the management console, select option 1 (Configuration Menu), then select option 4 (console menu), then check the setting of option 5 (Http). If setting is OFF, then web management is disabled. If setting is ON, select option 5 (Http) to toggle setting to OFF.

To avoid unnecessary handling of HTTP requests by Cisco routers running IOS, disable the HTTP server by applying:

```
no ip http server
```

while in global configuration mode. If HTTP service is needed, consider restricting access by applying an access list command.

Additional Workarounds for Handling "CodeRed" Traffic

Utilize the NBAR feature in supported Cisco IOS Software versions to aid in "Code Red" traffic identification and mitigation. This is discussed in detail at http://www.cisco.com/warp/public/63/nbar_acl_codered.shtml. This workaround is applicable in Cisco IOS Software Version 12.1(5)T and later for many platforms.

Classify inbound Code Red traffic with the class-based marking feature in IOS.

```
Router(config)#class-map match-any http-codered
Router(config-cmap)#match protocol http url "**default.ida*"
Router(config-cmap)#match protocol http url "**cmd.exe*"
Router(config-cmap)#match protocol http url "**root.exe*"
```

Mark inbound Code Red traffic with a policy map.

Once the inbound traffic has been classified as Code Red, it can be marked with a specific DSCP. For this example, a decimal value of '1' is used as it is unlikely that any other traffic would be marked with this DSCP.

```
Router(config)#policy-map mark-inbound-http-codered
Router(config-pmap)#class http-codered
Router(config-pmap)#set ip dscp 1
```

Apply the service policy to the 'outside' interface so inbound traffic will be marked.

```
Router(config)#int e 0/0
Router(config-if)#service-policy input mark-inbound-http-codered
```

Block marked Code Red attempts with an ACL. The ACL will match on the DSCP value of '1' that was marked as the Code Red attempt entered in the box.

```
Router(config)#access-list 105 deny ip any any dscp 1 log
Router(config)#access-list 105 permit ip any any
```

Apply it outbound on the 'inside' interface where the target web servers are.

```
Router(config)#int e 0/1
Router(config-if)#ip access-group 105 out
```

Workaround for Cisco Cache/Content Engine Products

Additionally, Cisco Content Engines or Cisco Cache Engines can be configured to block "Code Red" associated traffic with a filter ruleset as described below.

Cache Engine/Content Engine

```
rule enable
rule block url-regex .*\.ida.*
```

Fixed Software

Microsoft has made a patch available for affected systems at <http://www.microsoft.com/technet/security/Bulletin/MS01-033.msp>



Cisco is providing the same patch at <http://www.cisco.com/cgi-bin/Software/Tablebuild/doftp.pl?ftpfile=cisco/voice/callmgr/win-IIS-SecurityUpdate-2.exeswtype=FCScode=size=246296>.

Documentation is available at <http://www.cisco.com/cgi-bin/Software/Tablebuild/doftp.pl?ftpfile=cisco/voice/callmgr/win-IIS-SecurityUpdate-Readme-2.htm swtype=FCScode=size=4541>.

The Cisco Building Broadband Service Manager is documented separately at <http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/bbsm50/urgent.htm>.

The Cisco CSS 11000 Content Service Switch memory allocation error is fixed in versions R3.10 B78s, R4.01 B41s, R4.10 B21s, R5.0 B8s, and R5.01 B5.

Cisco is providing software patches for the IP/VC 3510 and IP/VC 3540 products at <http://www.cisco.com/cgi-bin/tablebuild.pl/ipvc>.

The Cisco 67x series is vulnerable partially due to previously documented vulnerabilities at <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20001204-cbos>.

Exploitation and Public Announcements

This issue is being exploited actively and has been discussed in numerous public announcements and messages. References include:

- <http://www.cert.org/advisories/CA-2001-19.html>
- <http://www.eeye.com/html/Research/Advisories/AD20010618.html>

The additional workarounds in this advisory utilizing the NBAR feature have been provided through the work of Randall Benn.

URL

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010720-code-red-worm>

Revision History

Revision 2.3	2001-November-01	Updated Additional Workarounds for Handling "CodeRed" Traffic section
Revision 2.2	2001-August-11	Updated Workaround section and Affected Products
Revision 2.1	2001-August-08	Updated Workaround section and Affected Products
Revision 2.0	2001-July-31	Updated to include CSS 11000 and old network management platforms.

Revision 1.1	2001-July-23	Made Microsoft patch URL visible, and changed relative links to fully qualified.
Revision 1.0	2001-July-20	Initial public release.

Legal Disclaimer

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 is an uncontrolled copy, and may lack important information or contain factual errors. The information in this document is intended for end-users of Cisco products.

Information For Small Business Midsize Business Service Provider Executives Industries > Marketplace Contacts Contact Cisco Find a Reseller	News & Alerts Newsroom Blogs Field Notices Security Advisories Technology Trends Cloud Internet of Things (IoT) Mobility Software Defined Networking (SDN)	Support Downloads Documentation Communities DevNet Learning Network Support Community Video Portal >	About Cisco Investor Relations Corporate Social Responsibility Environmental Sustainability Tomorrow Starts Here Our People Careers Search Jobs Life at Cisco Programs Cisco Designated VIP Program Cisco Powered Financing Options
--	---	--	--