

Table of Contents

<u>Cisco Security Advisory: IOS Heap-based Overflow Vulnerability in System Timers</u>	1
<u>Document ID: 68064</u>	1
<u>Revision 1.2</u>	1
<u>Last Updated 2005 November 4 1400 UTC (GMT)</u>	1
<u>For Public Release 2005 November 2 1600 UTC (GMT)</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Affected Products</u>	1
<u>Background Information Regarding Heap Overflows</u>	2
<u>Details</u>	3
<u>Impact</u>	3
<u>Software Versions and Fixes</u>	3
<u>Obtaining Fixed Software</u>	12
<u>Customers with Service Contracts</u>	12
<u>Customers using Third-party Support Organizations</u>	13
<u>Customers without Service Contracts</u>	13
<u>Workarounds</u>	13
<u>Exploitation and Public Announcements</u>	14
<u>Status of This Notice: FINAL</u>	14
<u>Distribution</u>	14
<u>Revision History</u>	14
<u>Cisco Security Procedures</u>	15

Cisco Security Advisory: IOS Heap-based Overflow Vulnerability in System Timers

Document ID: 68064

Revision 1.2

Last Updated 2005 November 4 1400 UTC (GMT)

For Public Release 2005 November 2 1600 UTC (GMT)

Please provide your feedback on this document.

Summary
Affected Products
Background Information Regarding Heap Overflows
Details
Impact
Software Versions and Fixes
Obtaining Fixed Software
Workarounds
Exploitation and Public Announcements
Status of This Notice: FINAL
Distribution
Revision History
Cisco Security Procedures

Summary

The Cisco Internetwork Operating System (IOS) may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

Cisco has made free software available that includes the additional integrity checks for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml>.

Cisco is not aware of any active exploitation of this vulnerability. This advisory documents changes to Cisco IOS® as a result of continued research related to the demonstration of the exploit for another vulnerability which occurred in July 2005 at the Black Hat USA Conference. Cisco addressed the IPv6 attack vector used in that demonstration in a separate advisory published on July 29, 2005.

Affected Products

This security advisory applies to all Cisco products that run Cisco IOS Software. Any version of Cisco IOS prior to the versions listed in the Fixed Software table below may be susceptible to heap overflow exploitation.

Cisco IOS XR is not affected.

To determine the software running on a Cisco product, log in to the device and issue the **show version** command to display the system banner. Cisco IOS Software will identify itself as "Internetwork Operating System Software" or simply "IOS". On the next line of output, the image name will be displayed between parentheses, followed by "Version" and the IOS release name. Other Cisco devices will not have the **show version** command or will give different output.

The following example identifies a Cisco product running IOS release 12.3(6) with an installed image name of C3640-I-M:

```
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-I-M), Version 12.3(6), RELEASE SOFTWARE (fc3)
```

The next example shows a product running IOS release 12.3(11)T3 with an image name of C3845-ADVIPSERVICESK9-M:

```
Cisco IOS Software, 3800 Software (C3845-ADVIPSERVICESK9-M), Version 12.3(11)T3, RELEASE S
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
```

Additional information about Cisco IOS release naming can be found at <http://www.cisco.com/warp/public/620/1.html>.

No other Cisco products are currently known to be affected by the vulnerability addressed in this advisory.

Background Information Regarding Heap Overflows

As this security advisory pertains to heap overflows, the following additional information is provided to aid in understanding the terminology used in this advisory.

RFC 2828 defines a vulnerability as "A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy." The threat from any particular vulnerability in a system or a protocol depends on the ease and likelihood in which the normal operations of a system can be disrupted or compromised. In order to minimize the threat, each possible attack vector for a particular vulnerability should either be mitigated with protections which may prevent the circumstances required for exploitation or remediated with software that no longer contains the vulnerability.

Many forms of malicious software, commonly known as "exploits", contain a payload that seeks to disrupt or compromise a system delivered through well-known attack vectors for particular vulnerabilities. In cases where it is likely that unpatched vulnerable systems exist, counter-measures are often employed to attempt to block any and all attack vectors to minimize the threat of successful exploitation. One popular attack method often found in the payload of exploits is known as a buffer overflow.

A heap-based overflow is a type of buffer overflow against a data structure residing within the memory heap. The memory heap is a section of system memory used by the operating system of the device to satisfy the dynamic data storage requirements for currently running processes. In a successful heap-based overflow, the operating system fails to enforce bounds checking on a buffer, thus allowing for the possibility of overwriting adjacent locations in system memory.

The threat from buffer overflows, like the one described in this advisory, may be remediated in multiple ways. One way is to remove the particular attack vector so that it no longer exists. Another way is to employ protections in the underlying system to minimize the consequences of any future buffer overflow

Cisco Security Advisory: IOS Heap-based Overflow Vulnerability in System Timers

vulnerabilities that may be discovered.

Details

Cisco IOS may be susceptible to remote code execution through attack vectors such as specific heap-based overflows in which internal operating system timers may execute arbitrary code from portions of memory that have been overwritten via exploitation.

In many cases, a heap-based overflow in Cisco IOS will simply corrupt system memory and trigger a system reload when detected by the "Check Heaps" process, which constantly monitors for such memory corruption. In a successful attack against an appropriate heap-based overflow, it is possible to achieve code execution without the device crashing immediately.

Cisco has devised counter-measures by implementing extra checks to enforce the proper integrity of system timers. This extra validation should reduce the possibility of heap-based overflow attack vectors achieving remote code execution.

These improvements have been documented in Cisco Bug ID CSCei61732. (registered customers only) .

Impact

Successful exploitations of heap-based buffer overflow vulnerabilities in Cisco IOS software often result in a Denial of Service because the exploit causes the router to crash and reload due to inconsistencies in running memory. In some cases it is possible to overwrite areas of system memory and execute arbitrary code from those locations. In the event of successful remote code execution, device integrity will have been completely compromised.

Software Versions and Fixes

When considering software upgrades, please also consult http://www.cisco.com/en/US/products/products_security_advisories_listing.html 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") for assistance.

Each row of the Cisco IOS software table (below) 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 (the "First Fixed Release") and the anticipated date of availability for each are listed in the "Rebuild" and "Maintenance" columns. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

For further information on the terms "Rebuild" and "Maintenance," please consult the following URL: <http://www.cisco.com/warp/public/620/1.html>.

Major Release	Availability of Repaired Releases	
	Rebuild	Maintenance

Affected 12.0-Based Release		
12.0	12.0(28d)	
12.0DA	Vulnerable; migrate to 12.2(12)DA9 or later	
12.0DB	Vulnerable; migrate to 12.3(14)T4 or later	
12.0DC	Vulnerable; migrate to 12.2(15)BC2i or later	
12.0S	12.0(28)S5	
	12.0(30)S4	
	12.0(31)S1	
12.0SC	Vulnerable; migrate to 12.2(15)BC2i or later	
12.0SL	Vulnerable; migrate to 12.0(31)S1 or later	
12.0SP	Vulnerable; migrate to 12.0(31)S1 or later	
12.0ST	Vulnerable; migrate to 12.0(31)S1 or later	
12.0SX	Vulnerable; contact TAC	
12.0SZ	Vulnerable; migrate to 12.0(31)S1 or later	
12.0T	Vulnerable; migrate to 12.1(27b) or later	
12.0W5	12.0(25)W5-27d	
	12.0(28)W5-30b	
	12.0(28)W5-32a	
12.0WC	12.0(5)WC13	
12.0XA	Vulnerable; migrate to 12.1(27b) or later	
12.0XB	Vulnerable; migrate to 12.1(27b) or later	
12.0XC	Vulnerable; migrate to 12.1(27b) or later	
12.0XD	Vulnerable; migrate to 12.1(27b) or later	
12.0XE	Vulnerable; migrate to 12.1(26)E3 or later	
12.0XF	Vulnerable; migrate to 12.1(27b) or later	
12.0XG	Vulnerable; migrate to 12.1(27b) or later	
12.0XH	Vulnerable; migrate to 12.1(27b) or later	
12.0XI	Vulnerable; migrate to 12.1(27b) or later	
12.0XJ	Vulnerable; migrate to 12.1(27b) or later	
12.0XK	Vulnerable; migrate to 12.2(31) or later	
12.0XL	Vulnerable; migrate to 12.2(31) or later	
12.0XM	Vulnerable; migrate to 12.1(27b) or later	
12.0XN	Vulnerable; migrate to 12.1(27b) or later	
12.0XQ	Vulnerable; migrate to 12.1(27b) or later	

12.0XR	Vulnerable; migrate to 12.2(31) or later	
12.0XS	Vulnerable; migrate to 12.1(26)E3 or later	
12.0XV	Vulnerable; migrate to 12.1(27b) or later	
Affected 12.1–Based Release	Rebuild	Maintenance
12.1	12.1(27b)	
12.1AA	Vulnerable; migrate to 12.2(31) or later	
12.1AX	Vulnerable; for c3750–ME, migrate to 12.2(25)EY3 or later. For c2970 and 3750, migrate to 12.2(25)SEB4, 12.2(25)SEC2, 12.2(25)SED or later.	
12.1AY	Vulnerable; migrate to 12.1(22)EA4a, 12.1(22)EA5a, 12.2(22)EA6 or later	
12.1AZ	Vulnerable; migrate to 12.1(22)EA4a, 12.1(22)EA5a, 12.2(22)EA6 or later	
12.1CX	Vulnerable; migrate to 12.2(31) or later	
12.1DA	Vulnerable; migrate to 12.2(12)DA9 or later	
12.1DB	Vulnerable; migrate to 12.3(14)T4 or later	
12.1DC	Vulnerable; migrate to 12.3(14)T4 or later	
12.1E	12.1(8b)E20	
	12.1(13)E17	
	12.1(23)E4	
	12.1(26)E3	
12.1EA	12.1(22)EA4a	12.1(22)EA6
	12.1(22)EA5a	
12.1EB	12.1(26)EB1	
12.1EC	Vulnerable; migrate to 12.2(15)BC2i or later	
12.1EO	12.1(20)EO3, available 11/30/05	
12.1EU	Vulnerable; migrate to 12.2(20)EU2 or later	
12.1EV	Vulnerable; migrate to 12.2(26)SV1 or later	
12.1EW	12.1(12c)EW4	
	12.1(13)EW4	
	12.1(19)EW3	
	12.1(20)EW4	
12.1EX	Vulnerable; migrate to 12.1(26)E3 or later	
12.1EY	Vulnerable; migrate to 12.1(26)E3 or later	

12.1EZ	Vulnerable; migrate to 12.1(26)E3 or later	
12.1T	Vulnerable; migrate to 12.2(31) or later	
12.1XA	Vulnerable; migrate to 12.2(31) or later	
12.1XB	Vulnerable; migrate to 12.2(31) or later	
12.1XC	Vulnerable; migrate to 12.2(31) or later	
12.1XD	Vulnerable; migrate to 12.2(31) or later	
12.1XE	Vulnerable; migrate to 12.1(26)E3 or later	
12.1XF	Vulnerable; migrate to 12.3(16) or later	
12.1XG	Vulnerable; migrate to 12.3(16) or later	
12.1XH	Vulnerable; migrate to 12.2(31) or later	
12.1XI	Vulnerable; migrate to 12.2(31) or later	
12.1XJ	Vulnerable; migrate to 12.3(16) or later	
12.1XL	Vulnerable; migrate to 12.3(16) or later	
12.1XM	Vulnerable; migrate to 12.3(16) or later	
12.1XP	Vulnerable; migrate to 12.3(16) or later	
12.1XQ	Vulnerable; migrate to 12.3(16) or later	
12.1XR	Vulnerable; migrate to 12.3(16) or later	
12.1XS	Vulnerable; migrate to 12.2(31) or later	
12.1XT	Vulnerable; migrate to 12.3(16) or later	
12.1XU	Vulnerable; migrate to 12.3(16) or later	
12.1XV	Vulnerable; migrate to 12.3(16) or later	
12.1XW	Vulnerable; migrate to 12.2(31) or later	
12.1XX	Vulnerable; migrate to 12.2(31) or later	
12.1XY	Vulnerable; migrate to 12.2(31) or later	
12.1YA	Vulnerable; migrate to 12.3(16) or later	
12.1YB	Vulnerable; migrate to 12.3(16) or later	
12.1YC	Vulnerable; migrate to 12.3(16) or later	
12.1YD	Vulnerable; migrate to 12.3(16) or later	
12.1YE	Vulnerable; migrate to 12.3(16) or later	
12.1YF	Vulnerable; migrate to 12.3(16) or later	
12.1YH	Vulnerable; migrate to 12.3(16) or later	
12.1YI	Vulnerable; migrate to 12.3(16) or later	
12.1YJ	Vulnerable; migrate to 12.1(22)EA4a, 12.1(22)EA5a, 12.1(22)EA6 or later	
Affected 12.2–Based	Rebuild	Maintenance

Release		
12.2	12.2(12m)	
	12.2(17f)	
	12.2(23f)	
	12.2(26b)	
	12.2(27b)	
	12.2(28c)	
	12.2(29a)	12.2(31)
12.2B	Vulnerable; migrate to 12.3(14)T4 or later	
12.2BC	12.2(15)BC2i	
12.2BX	Vulnerable; migrate to 12.3(7)XI7, available 15–Nov–2005	
12.2BY	Vulnerable; migrate to 12.3(14)T4 or later	
12.2BZ	Vulnerable; migrate to 12.3(7)XI7, available 15–Nov–2005	
12.2CX	Vulnerable; migrate to 12.2(15)BC2i or later	
12.2CY	Vulnerable; migrate to 12.2(15)BC2i or later	
12.2CZ	12.2(15)CZ3, available 3–Nov–2005	
12.2DA	12.2(10)DA4	
	12.2(12)DA9	
12.2DD	Vulnerable; migrate to 12.3(14)T4 or later	
12.2DX	Vulnerable; migrate to 12.3(14)T4 or later	
12.2EU	12.2(20)EU2	
12.2EW	12.2(18)EW5	
	12.2(20)EW3	
12.2EWA	12.2(20)EWA3	
	12.2(25)EWA3	
12.2EX		12.2(25)EX, available 03–Nov–2005
12.2EY	12.2(25)EY3	Migrate to 12.2(25)SED
12.2EZ	Vulnerable; migrate to 12.2(25)SEC2, 12.2(25)SED or later	
12.2FX		12.2(25)FX, available 07–Nov–2005
12.2FY		12.2(25)FY

12.2JA	Vulnerable; migrate to 12.3(7)JA1 or later	
12.2JK	12.2(15)JK5	
12.2MB	12.2(4)MB13c	
12.2MC	12.2(15)MC2e	
12.2S	12.2(14)S15	
	12.2(18)S10	
	12.2(20)S9	
	12.2(25)S6	
	12.2(30)S1, available 14–Nov–2005	
12.2SBC		12.2(27)SBC
12.2SE	12.2(25)SEB4	12.2(25)SED
	12.2(25)SEC2	
12.2SG		12.2(25)SG
12.2SO	12.2(18)SO4	
12.2SU	Vulnerable; migrate to 12.3(14)T4 or later	
12.2SV	12.2(26)SV1	
	12.2(27)SV1, available 15–Nov–2005	
12.2SW		12.2(25)SW4
12.2SX	Vulnerable; migrate to 12.2(17d)SXB10 or later	
12.2SXA	Vulnerable; migrate to 12.2(17d)SXB10 or later	
12.2SXB	12.2(17d)SXB10	
12.2SXD	12.2(18)SXD6	
12.2SXE	12.2(18)SXE3	
12.2SXF		12.2(18)SXF
12.2SY	Vulnerable; migrate to 12.2(17d)SXB10 or later	
12.2SZ	Vulnerable; migrate to 12.2(25)S6 or later	
12.2T	12.2(15)T17	
12.2TPC	12.2(8)TPC10a, available TBD	
12.2XA	Vulnerable; migrate to 12.3(16) or later	
12.2XB	Vulnerable; migrate to 12.3(16) or later	

12.2XC	Vulnerable; migrate to 12.3(14)T4 or later
12.2XD	Vulnerable; migrate to 12.3(16) or later
12.2XE	Vulnerable; migrate to 12.3(16) or later
12.2XF	Vulnerable; migrate to 12.2(15)BC2i or later
12.2XG	Vulnerable; migrate to 12.3(16) or later
12.2XH	Vulnerable; migrate to 12.3(16) or later
12.2XI	Vulnerable; migrate to 12.3(16) or later
12.2XJ	Vulnerable; migrate to 12.3(16) or later
12.2XK	Vulnerable; migrate to 12.3(16) or later
12.2XL	Vulnerable; migrate to 12.3(16) or later
12.2XM	Vulnerable; migrate to 12.3(16) or later
12.2XN	Vulnerable; migrate to 12.3(16) or later
12.2XQ	Vulnerable; migrate to 12.3(16) or later
12.2XR	12.2(2)XR and 12.2(4)XR vulnerable, migrate to 12.3(16) or later
	12.2(15)XR vulnerable; migrate to 12.3(7)JA1
12.2XS	Vulnerable; migrate to 12.3(16) or later
12.2XT	Vulnerable; migrate to 12.3(16) or later
12.2XU	Vulnerable; migrate to 12.3(16) or later
12.2XV	Vulnerable; migrate to 12.3(16) or later
12.2XW	Vulnerable; migrate to 12.3(16) or later
12.2YA	12.2(4)YA11, available TBD
12.2YB	Vulnerable; migrate to 12.3(16) or later
12.2YC	Vulnerable; migrate to 12.3(16) or later
12.2YD	Vulnerable; migrate to 12.3(14)T4 or later
12.2YE	Vulnerable; migrate to 12.2(25)S6 or later
12.2YF	Vulnerable; migrate to 12.3(16) or later
12.2YG	Vulnerable; migrate to 12.3(16) or later
12.2YH	Vulnerable; migrate to 12.3(16) or later
12.2YJ	Vulnerable; migrate to 12.3(16) or later
12.2YK	Vulnerable; migrate to 12.3(14)T4 or later
12.2YL	Vulnerable; migrate to 12.3(14)T4 or later
12.2YM	Vulnerable; migrate to 12.3(14)T4 or later
12.2YN	Vulnerable; migrate to 12.3(14)T4 or later
12.2YO	

	Vulnerable; migrate to 12.2(17d)SXB10 or later	
12.2YP	Vulnerable; migrate to 12.3(16) or later	
12.2YQ	Vulnerable; migrate to 12.3(14)T4 or later	
12.2YR	Vulnerable; migrate to 12.3(14)T4 or later	
12.2YS		12.2(15)YS
12.2YT	Vulnerable; migrate to 12.3(16) or later	
12.2YU	Vulnerable; migrate to 12.3(14)T4 or later	
12.2YV	Vulnerable; migrate to 12.3(14)T4 or later	
12.2YW	Vulnerable; migrate to 12.3(14)T4 or later	
12.2YX	Vulnerable; migrate to 12.3(14)T4 or later	
12.2YY	Vulnerable; migrate to 12.3(14)T4 or later	
12.2YZ	Vulnerable; migrate to 12.2(25)S6 or later	
12.2ZA	Vulnerable; migrate to 12.2(17d)SXB10 or later	
12.2ZB	Vulnerable; migrate to 12.3(14)T4 or later	
12.2ZC	Vulnerable; migrate to 12.3(14)T4 or later	
12.2ZD		12.2(13)ZD4
12.2ZE	Vulnerable; migrate to 12.3(16) or later	
12.2ZF	Vulnerable; migrate to 12.3(14)T4 or later	
12.2ZG	Vulnerable; migrate to 12.3(8)YG3 or later for SOHO9x migrate to 12.3(2)XA5 or later for c83x	
12.2ZH	12.2(13)ZH8, available TBD	
12.2ZJ	Vulnerable; migrate to 12.3(14)T4 or later	
12.2ZL	Vulnerable; migrate to 12.3(4)XK4 or later for c17xx migrate to 12.4(3a) or later for c3200 migrate to 12.3(7)XR6 or later for ICS7750	
12.2ZN	Vulnerable; migrate to 12.3(14)T4 or later	
12.2ZP	Vulnerable; migrate to 12.3(14)T4 or later	
Affected 12.3–Based Release	Rebuild	Maintenance
12.3	12.3(3i)	
	12.3(5f)	
	12.3(6f)	
	12.3(9e)	

	12.3(10e)	
	12.3(12e)	
	12.3(13b)	
	12.3(15b)	12.3(16)
12.3B	Vulnerable; migrate to 12.3(14)T4 or later	
12.3BC	12.3(9a)BC7	
	12.3(13a)BC1	
12.3BW	Vulnerable; migrate to 12.3(14)T4 or later	
12.3JA	12.3(2)JA5	
	12.3(4)JA1	
	12.3(7)JA1	
12.3JK	12.3(2)JK1	
12.3JX	12.3(7)JX	
12.3T	12.3(7)T12	
	12.3(8)T11	
	12.3(11)T8	
	12.3(14)T4	
12.3TPC	12.3(4)TPC11a	
12.3XA	12.3(2)XA5, available TBD	
12.3XB	Vulnerable; migrate to 12.3(14)T4 or later	
12.3XC	12.3(2)XC4	
12.3XD	Vulnerable; migrate to 12.3(14)T4 or later	
12.3XE	12.3(4)XE4, available TBD	
12.3XF	Vulnerable; migrate to 12.3(14)T4 or later	
12.3XG	12.3(4)XG5	
12.3XH	Vulnerable; migrate to 12.3(14)T4 or later	
12.3XI	12.3(7)XI7, available 15–Nov–2005	
12.3XJ	Vulnerable; migrate to 12.3(11)YF4 or later	
12.3XK	12.3(4)XK4	
12.3XM	Vulnerable; migrate to 12.3(14)T4 or later	
12.3XQ	Vulnerable; migrate to 12.4(3a) or later	
12.3XR	12.3(7)XR6	
12.3XS	Vulnerable; migrate to 12.4(3a) or later	

12.3XU	Vulnerable; migrate to 12.4(2)T1 or later	
12.3XW	Vulnerable; migrate to 12.3(11)YF4 or later	
12.3XX	Vulnerable; migrate to 12.4(3a) or later	
12.3XY	Vulnerable; migrate to 12.3(14)T4 or later	
12.3YA	Vulnerable; migrate to 12.4(3a) or later for C828; migrate to 12.3(8)YG3 or later for SOHO9x, C83x	
12.3YD	Vulnerable; migrate to 12.4(2)T1 or later	
12.3YF	12.3(11)YF4	
12.3YG	12.3(8)YG3	
12.3YH	Vulnerable; migrate to 12.3(8)YI3 or later	
12.3YI	12.3(8)YI3	
12.3YJ	12.3(14)YQ3	
12.3YK	12.3(11)YK2	
12.3YQ	12.3(14)YQ3	
12.3YS	12.3(11)YS1	
12.3YT	12.3(14)YT1	
12.3YU	12.3(14)YU1	
Affected 12.4–Based Release	Rebuild	Maintenance
12.4	12.4(1b)	
	12.4(3a)	12.4(5)
12.4MR		12.4(2)MR1
12.4T	12.4(2)T1	12.4(4)T
12.4XA		12.4(2)XA
12.4XB		12.4(2)XB, available 18–Nov–2005

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 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

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.

See <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.

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>.

Workarounds

There are no workarounds or configuration changes that will implement counter-measures equivalent to the increased integrity checks on system timers that have been introduced. In order to reduce the potential for system timer-related arbitrary code execution, an IOS upgrade is necessary.

Successful exploitation requires an appropriate attack vector such as the vulnerability described in <http://www.cisco.com/warp/publics/707/cisco-sa-20050729-ipv6.shtml>. Vulnerability specific workarounds and mitigation steps may help to minimize the threat to the device by removing or minimizing the available attack vectors, but the device could still be vulnerable through any other attack vectors in which a software fix or mitigation has not been implemented.

Exploitation and Public Announcements

The Cisco PSIRT is not aware of malicious use of the vulnerability described in this advisory. Exploit code exists for this vulnerability. It was used in a demonstration by Mike Lynn on July 27, 2005 at the Black Hat USA 2005 security conference where a heap overflow via an IPv6 attack vector achieved remote code execution. The IPv6 attack vector was addressed separately in a Cisco security advisory released on July 29, 2005.

Status of This Notice: FINAL

THIS ADVISORY IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTY OF MERCHANTABILITY. YOUR USE OF THE INFORMATION ON THE ADVISORY OR MATERIALS LINKED FROM THE ADVISORY IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS NOTICE AT ANY TIME.

A stand-alone copy or paraphrase of the text of this security advisory 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 is posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.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
- first-teams@first.org (includes CERT/CC)
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

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 1.2	4-Nov-2005	Further clarified obtaining fixed software section, updated fixed software for 12.2EWA, 12.2SW, 12.4, 12.4T
Revision 1.1	3-Nov-2005	Clarified obtaining fixed software
	2-Nov-2005	section Initial public release

Revision		
1.0		

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 © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Nov 04, 2005

Document ID: 68064
