

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

Revision 1.0

[2005 11 16 16:00 UTC \(GMT\)](#)

[2005 11 16 16:00 UTC \(GMT\)](#)

---

© 2005 Cisco Systems, Inc.

000000

000000

000000

000000

000000

000000

000000

000000

000000

000000

000000

000000

000000

000000

Cisco Internetwork Operating System (IOS)

000000

000000

000000

<http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml>

000000

7 2005 11 16 16:00 UTC (GMT)

000000

IOS 000000

000000

000000

000000







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	
<b>Affected 12.1-Based Release</b>	<b>Rebuild</b>	<b>Maintenance</b>
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	
<b>Affected 12.2-Based Release</b>	<b>Rebuild</b>	<b>Maintenance</b>
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	
	12.2(25)EWA4	
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
		12.2(25)SW4a
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	
<b>Affected 12.3-Based Release</b>	<b>Rebuild</b>	<b>Maintenance</b>
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	
<b>Affected 12.4-Based Release</b>	<b>Rebuild</b>	<b>Maintenance</b>
12.4	12.4(1b)	
	12.4(3a)	
12.4MR		12.4(2)MR1
12.4T	12.4(2)T1	
12.4XA		12.4(2)XA
12.4XB		12.4(2)XB, available 18-Nov-2005

ã;®æ£ã,½ãf•ãf^ã,|ã,§ã,çã®ã...¥æ%o<

ã®"ã¥'ç',ã,'æœ%oã®™ã,ã®Šã®çæš~

ã®"ã¥'ç',ã,'æœ%oã®™ã,ã®Šã®çæš~ã®-ã®é€šã,,ã®çμÇè-ã®šã®ã,Çã,'  
ã...¥æ%o<ã®—ã®|ã®ã®ã®ã®•ã®,ã®,ã®»ã®"ã,"ã®©ã®®ã®Šã®çæš~ã®-ã®ã,ã,ã,ã,ã®®ãf^ã  
ã,½ãf•ãf^ã,|ã,§ã,çã,»ãf³ã,¿ãf¼ã®<ã,®oã...¥æ%o<ã®™ã,ã®"ã®"ã®Çã®šã®ã®³¼ã®™ã®,  
<http://www.cisco.com>.

ã,ãf¼ãf%ãf^ãf¼ãf†ã,£ã®ã,μãf®ãf¼ãf^ã¼šç³¼ã,'ã®"ã^©ç""ã®ã®Šã®çæš~

ã,ã,ã,ã,ã f^ãf¼ãf^ãf¼ãf¼ã®æ£è|®è²©ã£²ã»£ç®†ã°—ã®ã,μãf¼ãf^ã,¹  
ãf—ãfãf®ã,ãf£ãf¼ã®ã®ã®©ã®ã,μãf¼ãf%ãf^ãf¼ãf†ã,£ã®ã,μãf®ãf¼ãf^ã¼šçç³¼ã®"ã»¥ã%o®ã  
ã,çãffãf—ã,°ãf-ãf¼ãf%ã®«é-çã®™ã,ã®æ"ã®,ã®—ã®'ã®|ã®ã®ã®ã®•ã®,ã®,ã®"ã®®æ"ã®æ

ã,ãf¼ãf^ã,"ã,¹ã¥'ç',ã,'ã®"ã^©ç""ã®šã®ã®,ã®,ã®Šã®çæš~

ã,ã,ã,ã,ã®ã,®oç'æZ¥è³¼ã...¥ã®—ã®ÿã®Çã,ã,ã,ã,ã®ã,μãf¼ãf^ã,¹ã¥'ç',ã,'ã®"ã^©ç""ã®,ã®,ã®ÿã®

Technical Assistance  
Center  
TAC

- +1 800 553 2447
- +1 408 526 7209
- é»à [tac@cisco.com](mailto:tac@cisco.com)

URL  
çµEç"±ã

psirt@cisco.com  
security-alert@cisco.com

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

<http://www.cisco.com/public/sw-license-agreement.html>

<http://www.cisco.com/center/sw-usingswc.shtml>

### á»žéç-

á»žéç-ã

IOS

<http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml>

«è»èç







## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。