# Multiple Vulnerabilities in Apache Struts 2 Affecting Cisco Products: 2017 æœˆ 9 æ—¥

Critical

**ã‚¢ãƒ‰ãƒ¬ã‚¹ã‚¿ã‚¤ãƒªãƒ³ã‚°ID :** cisco-sa-20170907-struts2

**å…¬é–‹æ—¥ :** 2017-09-07 21:00

**æœ€çµ‚æ›´æ–°æ—¥ :** 2017-10-23 20:27

**ãƒãƒ¼ã‚¸ãƧãƳ 1.12 :** Final

**å›žé¿ç– :** No workarounds available

**Cisco ãƒã,° ID :**

CVE-2017-9793
CVE-2017-9804
CVE-2017-9805

## æ—¥æœ¬èªžã«ã‚ˆã‚‹æ–‡å ±ã¯ã€è‹±èªžã«ã‚ˆã‚‹åŽŸæ–‡ã®å¾Œã«ç¶šãã¾ã™ã€‚

### æ¦‚è¦

2017 å¹´ 9 æœˆ 5 æ—¥ã€Apache ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢è²¡å›£ã¯ã€Apache Struts 2 ãƒ‘ãƒƒã‚±ãƼ¼ã‚¸ã® 3 ã¤ã®è„†å¼±æ€§ã‚’å…¬é–‹ã™ã‚‹ãƒ¡ãƒ¼ãƒªãƒ³ã‚°ãƪã‚¹ãƈã‚’ç™ºè¡Œã—ã¾ã—ãŸã€Apache ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢è²¡å›£ã¯ã“ã‚Œã‚‰ã®è„†å¼±æ€§ã® 1 ã¤ã‚’ *Critical*ã€ï1 ã¤ã‚’ *Medium*ã€ï1 ã¤ã‚’ *Low* ã®é‡ï¿½å¤§åº¦ã«å^†é¡žã—ã¾ã—ãŸ ã€,
ã“ã‚Œã‚‰ã®è„†å¼±æ€§ã®è©³ç´°ã«ã¤ã„ã¦ã¯ã€ã¾ã¨ã‚ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƪã®ã€è©³ç´°æƒ…å ±ã€‘ã®é …ã‚’å‚ç…§ã—ã¦ãã ã•ã„ã€,

ã‚·ã‚¹ãƳã®è¤‡æ•°ã®è£½å“ã«ã€Œã‚‰ã®è„†å¼±æ€§ã®å½±éŸ¿ã‚’å—ã‘ã‚‹ã‚ãƒ Apache Struts 2 ãƒ‘ãƒƒã‚±ãƼ¼ã‚¸ã€Œçµ„ã¿è¾¼ã¾ã¾ã¾ã¦ã„ã¾ã™ã€,

ã“ã®è„†å¼±æ€§ã®ä¸€æ£å^©ç”¨ã®å¯èƽæ€§ã‚’æ¤œå‡ºã™ã‚‹ã€Šç¡®èª ã®ãƒ«ãƼãƫ,ã‚’ä½¿ç”¨ã§ãã¾ã™ã€, Snort SID 44315 ã€Šã‚ˆã³ 44327 ï½ž 44330ã€,

ã“ã®ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƪã¯ã€æ¬¡ã®ãƪãƳã‚¯ã‚ˆã‚Šç¢ºèª ã§ã§ãã¾ã™ã€,
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170907-struts2

### è©²å½“è£½å“

è£½å“ã®ã“ã®è„†å¼±æ€§ã«ã‚ˆã‚‹å½±éŸ¿ã‚’å—ã‘ã‚‹ã‚ã©ã†ã‹ã‚’åˆ¤æ–ã™ã‚‹ã«ã¯ã€ã¾ã¨ã‚è„†å¼±æ€§ã¨ã®å¯¾è±¡è£½å“ã€ã®ã‚»ã‚¯ã‚·ãƧãƳã«ã‚ã‚‹ã€Šç¡®èª ã®ãƒ«ãƼãƫ,ã‚’ä½¿ç”¨ã—ã¦ãã ã•ã„ã€,
ã€Œè„†å¼±æ€§ã‚’å«ã‚“ã§ã„ãªã„ã“ã¨ãŒç¢ºèªã•ã‚Œã¦ã„ã‚‹è£½å“ã€ã«ã¯ã€è©²å½“è£½å“ã®ã‚»ã‚¯ã‚·ãƧãƳã«è¨˜è¼‰ã•ã‚Œã¦ã„ã‚‹è£½å“ã¯å«ã¾ã‚Œã¾ã›ã‚“ã€,

Cisco Bug ID ã‚’ç¤ºã—ã¾ã™ã€‚Bugs ã¯ Cisco Bug Search Tool
ã§æ¤œç´¢å¯¾è±¡ã§ã‚ã‚Šã€å˜ç”¨å¯èƒ½ã§ä¿®æ£ã•ã‚Œã‚Ÿã‚½ãƒ•ãƒˆã‚¦
ãƒªãƒªãƒ¼ã‚¹ã€ã‚»ã‚ãƒ¥ãƒªãƒ†ã‚£ã€©ãƒ¼ãƒ å›ºæœ‰ã®è¿½åŠ æƒ…å ±ãŒè¨˜è¼‰ã•

**æ³¨:**
ã€Œè„†å¼±æ€§ã‚Œã˜ã™ã‚‹ã€Œè„†å¼±æ€§ã‚’å«ã‚“ã§ã„ã¾ã™ã€‚
Struts ã‚’å«ã‚€ã‚·ã‚¹ãƒ†ãƒ ã¯ã¿ãªã•ã‚Œã¦ã•ã‚Œã¦ã„ã¾ã™ã€‚
ãƒªã‚¹ãƒˆã•ã‚Œã¦ã„ãªã„ã‚·ã‚¹ãƒ†ãƒ ã¯ Struts
ã¯å«ã¾ã‚Œã¦ã„ãŠã‚‰ãšã€ã¾ãŸã€ã‚Ÿã‚Œã£ã¦ã¯ã¯ã½±éŸ¿ã‚’å—ã‘ã¾ã›ã‚“ã€‚

## è„†å¼±æ€§ã®ã‚ã‚‹è£½å“

æ¬¡ã®è¡¨ã«ã€æœ¬ã‚¢ãƒ‰ãƒã‚¤ã‚¶ãƒªã«è¨˜è¼‰ã•ã‚Œã‚Ÿè„†å¼±æ€§ã®å½±éŸ¿ã‚’
è£½å“ã®å¾Œã®ã«ã‚¢ã‚¿ãƒƒãƒ—ãƒ‡ãƒ¼ãƒˆï¼‰ã«ã¯ã€å ´å ´ã€Œè£½å“ã«
Critical ã®ã‚ã‚‹è„†å¼±æ€§ CVE-2017-9805 *Apache Struts REST plug-in XML processing arbitrary code execution vulnerability* ã«è©²å½“ã—ã¾ã™ã€‚å…¬è¡¨æ™‚ç‚¹ã§ 4
ã¤ã®ã‚·ã‚¹ãƒ†ãƒ ã¯ CVE-2017-9805
ã«ã‚ˆã‚‹å½±éŸ¿ã‚’å—ã‘ã‚‹ã“ã¨ãŒç¢ºèªã•ã‚Œã¦ã„ã¾ã™ã€‚

ã‚·ã‚¹ãƒ†ãƒ ã¯ã€ã“ã®ã“ã¨ã«è¨˜è¼‰ã•ã‚Œã¦ã„ãªã„ã‚‚ã‚·ã‚¹ãƒ†ãƒ 
ãƒ•ã‚°ã«ä¿®æ£æ¸ˆã¿ã‚½ãƒ•ãƒˆã‚¦ã§ã‚¢ãƒƒãƒ—ãƒ‡ãƒ¼ãƒˆã•ã‚Œã¦ã„ã¾ã™ã€‚Bugs ã¯ã€
Cisco Bug Search Tool ã§æ¤œç´¢ã§ãã¾ã™ã€‚ã‚½ãƒ•ãƒˆã‚¦ã§ã‚¢ãƒƒãƒ—ãƒ‡ãƒ¼ãƒˆã•ã‚Œã¦ã„ã‚‹ Bugs
ã‚’ç¢ºèªã—ã¦ãã ã•ã„ã€‚æœ€æ–°æ–°ãƒªãƒªãƒ¼ã‚¹ã«ã¯ã¨ã¦ã•ã‚Œã¦ã„ã¾ã™ã€‚

| Product | Cisco Bug ID | Fixed Release Availability |
|---|---|---|
| **Network Management and Provisioning** | | |
| Cisco Digital Media Manager | CSCvf86117 | ä¿®æ£äº†å®šã•ã‚Œã¦ã„ãªã„ï¼ˆEoSWMï¼‰ï¼2016 å¹´ 8 æœˆ 19 æ—¥ï¼‰ |
| Cisco MXE 3500 Series Media Experience Enginesï¼ˆ*ï¼‰ | CSCvf86119 | ä¿®æ£äº†å®šã•ã‚Œã¦ã„ãªã„ï¼ˆEoSWMï¼‰ï¼2017 å¹´ 1 æœˆ 2 æ—¥ï¼‰ |
| **Voice and Unified Communications Devices** | | |
| Cisco Hosted Collaboration Solution for Contact | CSCvf86143 | |

| | | |
|---|---|---|
| Centerï¼ˆ*ï¼‰ | | |
| **Video, Streaming, TelePresence, and Transcoding Devices** | | |
| Cisco Video Distribution Suite for Internet Streamingï¼ˆVDS-ISï¼‰ï¼ˆ*ï¼‰ | CSCvf86124 | Struts 2.3.34 ã‚'ä½¿ç”¨ã—ã¦ã¦è£½å“ã‚'æ›´æ–°ï¼ˆ2017 å¹´ 9 月 29 æ—¥ï¼‰ |
| **Cisco Hosted Services** | | |
| Cisco Network Performance Analysisï¼ˆ*ï¼‰ | CSCvf86134 | Struts 2.3.34 ã‚'ä½¿ç”¨ã—ã¦ã¦è£½å“ã‚'æ›´æ–°ï¼ˆ2017 å¹´ 9 月 12 æ—¥ï¼‰ |

## è„†å¼±æ€§ã‚'å«ã‚“ã§ã„ãªã„ã“ã¨ãŒç¢ºèªã•ã•

ã‚·ã‚¹ãƒ†ãƒ ä»¥ä¸‹ã®è£½å“ã«ã‚‚ã“ã®è„†å¼±æ€§ãƒ•ãƒ©ã‚¤ã‚¢ã‚¦ã‚©ãƒ¼ãƒ«ã«ã¨ã‚‰ã‚Ÿè¨¼ã•ã‚Œã•ã

*Collaboration and Social Media*

- Cisco Unified MeetingPlace
- Cisco WebEx Meetings Server

*ã‚¨ãƒ³ãƒ‰ãƒ¦ãƒ¼ã‚¶ãƒ¯ãƒ©ã‚¤ã‚ºãƒ‰ã‚¢ãƒ—ãƒªã‚±ãƒ¼ã‚·ãƒ§ãƒ³*

- Cisco WebEx Management - SuperAdmin ã‚³ãƒ³ãƒˆãƒãƒ¼ãƒ« ãƒ‘ãƒ«

*ãƒ‡ãƒãƒƒã‚¯ãƒ¯ãƒ¼ã‚¯ã€
ã‚¢ãƒ—ãƒªã‚±ãƒ¼ã‚·ãƒ§ãƒ³ã€µãƒ¼ãƒ“ã‚¹ã€ã‚¯ãƒ©ã‚¦ãƒ‰ã€*

- Cisco Data Center Network Manager

*ãƒ‡ãƒãƒƒã‚¯ãƒ¯ãƒ¼ã‚¯ã€ã‚¯ãƒ©ã‚¤ã‚¢ãƒ³ãƒˆã€ã‚µãƒ¼ãƒãƒ¼ã€ã‚¯ãƒ©ã‚¦ãƒ‰ã€ãƒ¢ãƒã‚¤ãƒ«ã€ãƒ‡ãƒã‚¤ã‚¹*

- Cisco Identity Services Engineï¼ˆISEï¼‰
- Cisco Secure Access Control Systemï¼ˆACSï¼‰

*ãƒ‡ãƒãƒƒã‚¯ãƒ¯ãƒ¼ã‚¯ã€ç®¡ç†ã€¨ãƒ—ãƒãƒ¼ã‚¸ãƒ§ãƒ³ã€*

- Cisco Prime Access Registrar
- Cisco Prime Central for Service Provider

- Cisco Prime Collaboration Assurance
- Cisco Prime Collaboration Provisioning
- Cisco Prime Home
- Cisco Prime Infrastructure
- Cisco Prime LAN Management Solution - Solaris
- Cisco Prime License Manager
- Cisco Prime Network Registrar IP ã,¢ãƒ‰ãƒ¬ã,¹ ãƒžãƒ�ãƼã,¸ãƣï¼ˆIPAMï¼‰
- Cisco Prime Network
- Cisco Security Manager
- Cisco Smart Net Total Care - ãƒãƼã,«ãƒ« ã,³ãƬã,¯ã,¿ ã,¢ãƒ—ãƒ©ã,¤ã,¢ãƳã,¹
- Cisco Unified Intelligence Center

*ãƫãƼãƆã,£ãƳã,°ã�Šã,ˆã�³ã,¹ã,¤ãƒƒãƒ�ãƳã,° - ã,¨ãƳã,¿ãƼãƗãƩã,¤ã,ºã�Šã,ˆã�³ã,µãƼãƑã,¹ ãƗãƫãƒ�ã,¤ãƀãƼ*

- Cisco Broadband Access Center for Telco and Wireless

*éŸ³å£°ã�Šã,ˆã�³ãƦ ãƒ‹ãƒ•ã,¡ã,¤ãƒ‰ ã,³ãŸãƒ¥ãƒ‹ã,±ãƼã,·ãƧãƳ ãƒ‡ãƒ�ã,¤ã,¹*

- Cisco Business Edition 4000
- Cisco Emergency Responder
- Cisco Enterprise Chat and Email
- Cisco Finesse
- Cisco Hosted Collaboration Mediation Fulfillment
- Cisco MediaSense
- Cisco SocialMiner
- Cisco Unified Communications Manager IM & Presence Serviceï¼ˆæ—§ç§° CUPSï¼‰
- Cisco Unified Communications Manager
- Cisco Unified Contact Center Enterprise - Live Data server
- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- Cisco Unified Customer Voice Portal
- Cisco Unified E-Mail Interaction Manager
- Cisco Unified Intelligent Contact Management Enterprise
- Cisco Unified SIP Proxy ã,½ãƒ•ãƈã,¦ã,§ã,¢
- Cisco Unified Survivable Remote Site Telephony Manager
- Cisco Unified Web Interaction Manager
- Cisco Unity Connection
- Cisco Unity Express
- Cisco Virtualized Voice Browser

ãƒ“ãƒ‡ã‚ªã€�ã‚¹ãƒˆãƒªãƒ¼ãƒŸãƒ³ã‚°ã€€ãƒ†ãƒ¬ãƒ—ãƒ¬ã‚¼ãƒ³ãƒ†ãƒ¼ã‚·ãƒ§ãƒ³ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ãƒ¼ãƒ‰ã‚¦ã‚§ã‚¢ãƒ‡ãƒ¢ã‚¤

- Cisco Enterprise Content Delivery System (ECDS)

ã‚·ã‚¹ãƒ†ãƒ ãƒ»ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢

- Cisco Business Video Services Automation Software
- Cisco ã‚¯ãƒ©ã‚¦ãƒ‰ E ãƒ¡ãƒ¼ãƒ« ã‚»ã‚ãƒ¥ãƒªãƒ†ã‚£
- Cisco Cloud Web Security
- Cisco Context Service
- Cisco Deployment Automation Tool
- Cisco Network Device Security Assessment Service
- Cisco Partner Support Service 1.x
- Cisco Prime ã‚µãƒ¼ãƒ“ã‚¹ ã‚«ã‚¿ãƒã‚°
- Cisco Services Provisioning Platform
- Cisco Smart Net Total Care - Contracts Information System Process Controller
- Cisco Smart Net Total Care
- Cisco Spark
- Cisco Tidal Performance Analyzer
- Cisco Umbrella
- Cisco Unified Service Delivery ãƒ—ãƒ©ãƒƒãƒˆãƒ•ã‚©ãƒ¼ãƒ
- Cisco WebEx Meeting Center - Windows
- Cisco WebEx Network-Based Recording (NBR) Management

**è©³ç´°**

**Apache Struts REST Plug-In XML Processing Arbitrary Code Execution Vulnerability**

Apache Struts ã�® Representational State Transferï¼ˆRESTï¼‰ãƒ—ãƒ©ã‚°ã‚¤ãƒ³ã�®è„†å¼±æ€§ã�«ã‚ˆã‚Šã€èª�è¨¼ã•ã‚Œã¦ã„ã„ã‚

ã�“ã�®è„†å¼±æ€§ã¯ã€REST ãƒ—ãƒ©ã‚°ã‚¤ãƒ³ã¨è©²å½“ã‚½ãƒ•ãƒˆã‚¦ã‚§ã‚¢ã•ã‚¢ã•ã‚¢ã•

ã“ã®è„†å¼±æ€§ã«ã¯æ¬¡ã® CVE ID
ã€Œå‰²ã‚Šå½“ã¦ã¦ã„ã‚‰ã‚Œã¦ã„ã„ã¾ã™ã€‚CVE-2017-9805

ã“ã®è„†å¼±æ€§ã®ã‚»ãƥãƪãƣã‚£å½±éŸ¿è©•ä¾¡ï¼ˆSIRï¼‰ã¯ *Critical* ã§ã™ã€‚

**Apache Struts REST Plug-In Denial of Service Vulnerability**

Apache Struts ã® REST
ãƗãƩã‚°ã‚¤ãƳã®è„†å¼±æ€§ã«ã‚ˆã‚Šã€ãƪãƣã‚¯ã‚¨ã‚¹ãƈã«ã„ãã¤ã‚‚ã®ãƫãƣãƈãƗãƳãƈãŒ
ã‚·ã‚¹ãƈãƠ ã«ã‚µãƼãƗã‚Œã‚¹å¦¨å®³ï¼ˆDoSï¼‰çŠ¶æ…‹ã‚’ç™ºç”Ÿã•ã›ã‚‹å¯¯èƽæ€§ã

ã“ã®è„†å¼±æ€§ã¯ã€è©²å½“ã‚ãƗãƪã‚±ãƼã‚·ãƧãƳã® REST
ãƗãƩã‚°ã‚¤ãƳã® *XStream*
ãƩã‚¤ãƗãƩãƪã«ã‚ˆã‚‹ãƦãƼã‚¶æŒ‡å®šåš¥åŠ›ã®æ¤œè¨¼ã€Œä¸€å¿œå††å^†ã§ã‚ã‚‹ã“ã
æ”»æ’ƈè€…ã¯ã¯è©²å½“ã‚ã‚‹ãƆãƗ ã«å·§å¦™ã«ç´°å·¥ã—ã—Ÿ XML
ãƆãƼã‚¿ã‚’é€ä¿¡ã™ã‚‹ã“ã¨ã«ã‚ˆã‚Šã€ä¸€æ™‚çš„ãªã‚µãƼãƓã‚¹æ¶ˆè²»ã‚’å¼•ã
DoS çŠ¶æ…‹ã‚’å¼•ãèµ·ã“ã™ã“ã¨ãŒã§ãã¾ã™ã€‚

ã“ã®è„†å¼±æ€§ã«ã¯ CVE ID
ã€Œå‰²ã‚Šå½“ã¦ã¦ã„ã‚‰ã‚Œã¦ã„ã„ã¾ã™ã€‚CVE-2017-9793

ã“ã®è„†å¼±æ€§ã® SIR ã¯ *Medium* ã§ã™ã€‚

**Apache Struts URLValidator Resource Exhaustion Denial of Service Vulnerability**

Apache Struts ã® *URLValidator*
æ©Ÿèƒ½ã®è„†å¼±æ€§ã«ã‚ˆã‚Šã€ãƪãƣã‚¯ã‚¨ã‚¹ãƈã«ã„ãã¤ã‚‚ã®ãƫãƣãƈãƗãƳãƈãŒ

ã“ã®è„†å¼±æ€§ã¯ã€è©²å½“ã‚ãƽãƕãƈã‚¦ã‚§ã‚¢ã«ã„ *URLValidator*
æ©Ÿèƒ½ã‚’使ç”¨ã—ã—ã„ URL
ã‚’検証ã™ã‚‹éš›ã«ã€ãƆãƗ ã‚¦ã‚§ã‚¢ãƦãƼã‚¶æŒ‡å®šåš¥åŠ›ã®æ¤œè¨¼ã€Œä¸€å¿œå††å^†ã§ã‚ã‚‹ã“ã
æ”»æ’ƈè€…ã¯ã€Apache Struts
ã®è©²å½“ãƒãƼã‚¸ãƧãƳã‚’å^©ç”¨ã™ã‚‹ã“ã¨ã«ã‚ˆã‚Šã€ãƪãƣã‚¯ã‚¨ã‚¹ãƈã®ãƕã‚©ãƼãƗ
ãƕã‚£ãƼãƫãƕã‚‰å·§å¦™ã«ã€Œæ£¡è¡¨ç¾ï¼ˆregexï¼‰å‡¦ç†ã§ã *URLValidator*
ã‚Œé‎Žå‰°ã‚ªé‡‎ã‚® CPU

ãƒªã,½ãƒ¼ã,¹ã,'æ¶^è²»ã�™ã,‹æ�¡ä»¶ã,'å¼•ã��èµ·ã�"ã�—ã€�ã��ã�®çµ�果 DoS
çŠ¶æ…‹ã�«ã�ªã,‹å¯¯èƒ½æ€§ã�Œã�,ã,Šã�¾ã�™ã€,

ã�"ã�®è„†å¼±æ€§ã�«ã�¯æ¬¡ã�® CVE ID
ã�Œå‰²ã,Šå½"ã�¦ã,‰ã,Œã�¦ã�„ã�¾ã�™ã€, CVE-2017-9804

ã�"ã�®è„†å¼±æ€§ã�® SIR ã�¯ *Low* ã�§ã�™ã€,

## å›žé�¿ç–

ã�"ã,Œã,‰ã�®è„†å¼±æ€§ã�«å¯¾å‡¦ã�™ã,‹å›žé�¿ç–ã�¯ Cisco Bugs
ã�«è¨˜è¼‰ã�•ã,Œã€� Cisco Bug Search Tool
ã�§æ¤œç´¢ã�§ã��ã,‹ã,^ã�†ã�«ã�ªã,Šã�¾ã�™ã€,

## ä¿®æ£æ¸ˆã�¿ã,½ãƒ•ãƒˆã,¦ã,§ã,¢

è©²å½"ã,½ãƒ•ãƒˆã,¦ã,§ã,¢
ãƒªãƒªãƒ¼ã,¹ã�¸ã�®æ›´æ–°ãƒ—ãƒã,°ãƒ©ãƒ ã�¯å^©ç"¨å�¯èƒ½ã�«ã�ªã£ã�Ÿæ™,ç,¹ã�§å…¬é–‹ã€
Cisco Bugs ã�«è¨˜è¼‰ã�•ã,Œã�¾ã�™ã€, Cisco Bug Search Tool
ã,'ä½¿ç"¨ã�—ã�¦ã,¢ã,¯ã,»ã,¹ã�§ã��ã�¾ã�™ã€,

ã,·ã,¹ã,³ã�Œã"ã,Œã,‰ã�®è„†å¼±æ€§ã�«å¯¾å‡¦ã�™ã,‹ã,½ãƒ•ãƒˆã,¦ã,§ã,¢
ã,¢ãƒƒãƒ—ãƒ‡ãƒ¼ãƒˆã,'ãƒªãƒªãƒ¼ã,¹ã�—ã�Ÿéš›ã€�ã��ã�®ã,¢ãƒƒãƒ—ãƒ‡ãƒ¼ãƒˆã,'ã,¤ãƒ³ã,¹ãƒˆãƒ¼ãƒ«ãƒ¼ã,¸ãƒ§ãƒ³ã¨¨ãƒ•ã,£ãƒ¼ãƒãƒ£ ã,»ãƒƒãƒˆã�®ã�¿ã�¨ã�ªã,Šã�¾ã�™ã€,
ã��ã�®ã,ˆã�†ã�ªã,½ãƒ•ãƒˆã,¦ã,§ã,¢
ã,¢ãƒƒãƒ—ãƒ‡ãƒ¼ãƒ‰ã,'ã,¤ãƒ³ã,¹ãƒˆãƒ¼ãƒ«ã€�ãƒ€ã,¦ãƒ³ãƒãƒ¼ãƒ‰ã™ã,‹ã€�ã�¾ã�Ÿã¯ã€�ã
ãƒ©ã,¤ã,»ãƒ³ã,¹ã�®æ�¡é …ã�«å¾"ã�†ã"ã"¨ã�«å�Œæ„�ã��—ã�Ÿã"ã"¨ã�«ã�ªã,Šã�¾ã

https://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

ã�¾ã�Ÿã€�ã�Šå®¢æ§˜ã�Œã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã,'ãƒ€ã,¦ãƒ³ãƒãƒ¼ãƒ‰ã,‹ã,®ã¯ã€ã,
é€šå„¸ã€�ã"ã,Œã¯ä¥¥å‰©è³¼å…¥ã—ã—ã—Ÿã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã®ãƒ¡ãƒ³ãƒ†ãƒŠãƒ³ã,¹
ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã§ã™ã€, ç„¡å„Ÿã®ã,»ã,ãƒ¥ãƒªãƒ†ã,£ ã,½ãƒ•ãƒˆã,¦ã,§ã,¢
ã,¢ãƒƒãƒ—ãƒ‡ãƒ¼ãƒˆã«ã,ˆã€£ã€¦ã€ã€Šå®¢æ§˜ã«æ–°ã—ã„ã,½ãƒ•ãƒˆã,¦ã,§ã,¢
ãƒ©ã,¤ã,»ãƒ³ã,¹ã€è¿½åŠ ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ ãƒ•ã,£ãƒ¼ãƒãƒ£
ã,»ãƒƒãƒˆã€ã€ã¾ã€Ÿã€¯ãƒ¡ã,¸ãƒ£ãƒ¼ ãƒªãƒ"ã,¸ãƒ§ãƒ³
ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã€«å¯¾ã™ã,‹æ¨©é™ã€Œä»˜ä¸Žã•ã,Œã,‹ã"ã"¨ã¯ã€ã,Šã¾ã

ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã€®ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã,'æ¤œè¨Žã™ã,‹éš›ã«ã¯ã€ Cisco Security Advisories and Alerts

ãƒšãƒ¼ã‚¸ã�§å…¥æ‰‹ã�§ã��ã,‹ã,·ã,¹ã,³è£½å“�ã�®ã,¢ãƒ‰ãƒ�ã,¤ã,¶ãƒªã,’å®šæœŸçš„ã�«å�,ç…
ã,½ãƒªãƒ¥ãƒ¼ã,·ãƒ§ãƒ³ã,’ç¢ºèª�ã�—ã�¦ã��ã� ã�•ã�„ã€,

ã�„ã�šã,Œã�®å ´å�^ã,,ã€�ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã�™ã,‹ãƒ‡ãƒ�ã,¤ã,¹ã�«å��å^†ã�ªãƒ¡ãƒ¢ãƒª
ä¸�æ˜Žã�ªç‚¹ã�«ã�¤ã�„ã�¦ã�¯ã€�Cisco Technical Assistance
Centerï¼ˆTACï¼‰ã,,ã�—ã��ã�¯å¥‘ç´„ã�—ã�¦ã�„ã,‹ãƒ¡ãƒ³ãƒ†ãƒŠãƒ³ã,¹
ãƒ—ãƒãƒ¤ãƒ€ãƒ¼ã�«ã�Šå•�ã�„å�^ã,�ã�›ã��ã� ã�•ã�„ã€,

**ã,µãƒ¼ãƒ“ã,¹å¥‘ç´„ã,’ã�”å^©ç”¨ã�§ã��ã�ªã�„ã�Šå®¢æ§˜**

ã,·ã,¹ã,³ã�‹ã,‰ç›´æŽ¥è³¼å…¥ã�—ã�Ÿã�Œã,·ã,¹ã,³ã�®ã,µãƒ¼ãƒ“ã,¹å¥‘ç´„ã,’ã�”å^©ç”¨ã�„ã�Ÿã
ãƒ™ãƒ³ãƒ€ãƒ¼ã�‹ã,‰è³¼å…¥ã�—ã�Ÿä¿®æ£æ¸ˆã�¿ã,½ãƒ•ãƒˆã,¦ã,§ã,¢ã,’è³¼å…¥å…ˆã�‹ã,‰å
TAC ã�«é€£çµ¡ã�—ã�¦ã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã,’å…¥æ‰‹ã�—ã�¦ã��ã� ã�•ã�„ã€,
https://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

ç„¡å„Ÿã,¢ãƒƒãƒ—ã,°ãƒ¬ãƒ¼ãƒ‰ã�®å¯¾è±¡è£½å“�ã�§ã�,ã,‹ã�“ã��ã,’è¨¼æ˜Žã�—ã�¦ã�„ã
URL ã,’ã�”ç¨¿æ„�ã��ã� ã�•ã�„ã€,

**ä¿®æ£æ¸ˆã�¿ãƒªãƒªãƒ¼ã,¹**

è„†å¼±æ€§ã�Œå˜åœ¨ã�™ã,‹å„è£½å“�ã�®å½±éŸ¿ã,’å—ã�‘ã,‹ãƒªãƒªãƒ¼ã,¹ã�¨ä¿®æ£æ¸ˆã�¿
ã€Œè„†å¼±æ€§ã�Œå˜åœ¨ã�™ã,‹è£½å“�ã€�ã�®é …ã�§è£½å“�ã,’è˜åˆ¥ã�™ã,‹ Cisco
Bug ã,’å�,ç…§ã�—ã�¦ã��ã� ã�•ã�„ã€, Cisco Bugs ã�¯ã€� Cisco Bug Search Tool
ã�§æ¤œç´¢ã�§ã��ã�¾ã�™ã€,

## ä¸�æ£åˆ©ç”¨äº‹ä¾‹ã�¨å…¬å¼�ç™ºè¡¨

Cisco Product Security Incident Response
Teamï¼ˆPSIRTï¼‰ã�§ã�¯ã€�ã,·ã,¹ã,³è£½å“�ã�«å¯¾ã�™ã,‹ã�“ã�®è„†å¼±æ€§ã�®ä¸�æ£åˆ©ç

CVE-2017-9805 *Apache Struts REST plug-in XML processing arbitrary code execution vulnerability*
ã�«ã�¤ã�„ã�¦ã�¯ã€�ã,¢ã,¯ãƒ†ã,£ãƒ–ã�ªä¸�æ£åˆ©ç”¨ã�Œå ±å‘Šã•ã,Œã�¦ã�„ã¾ã™ã€
å…¬é–‹æ™‚ç‚¹ã�§ã“ã“ã«è¨˜è¼‰ã•ã,·ã,¹ãƒ†ãƒ ã,’è˜åˆ¥ã
ã,¢ã,¯ãƒ†ã,£ãƒ–ãƒ†ã,£ã�§ä¸»ã�«è¦³æ¸¬ã•ã,Œã�¦ã�„ã¾ã™ã€,

**å‡ºå…¸**

2017 å¹´ 9 æœˆ 5 æ—¥ã�« Apache
ã,½ãƒ•ãƒˆã,¦ã,§ã,¢è²¡å›£ã�¯æ¬¡ã�®ã,»ã,ãƒ¥ãƒªãƒ†ã,£æ…å ±ã�§ã“ã,Œã,‰ã�®è„†å¼±æ€§ã,’å…¬

- CVE-2017-9805ï¼š http://struts.apache.org/docs/s2-052.html
- CVE-2017-9804ï¼š http://struts.apache.org/docs/s2-050.html
- CVE-2017-9793ï¼š http://struts.apache.org/docs/s2-051.html

## URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170907-struts2

## æ”¹è¨‚å±¥æ´

â€”

| Version | Descripti |
|---|---|
| 1.12 | è„†å¼±æ€§ã‚’å«ã‚“ã§ã„ãªã„ã“ã¨ã‚’ç¢ºèªã•ã‚Œã‚Ÿè£½å“ãªã®ãƒªã‚¹ãƒˆã‚’ |
| 1.11 | ä¿®æ£ã«é–¢ã™ã‚‹æƒ…å ±ã‚’è¿½åŠ ã—ã€è„†å¼±æ€§ã®ã‚ã‚‹è£½å“ãƒªã‚¹ãƒˆã‚’<br>æ¦‚è¦ã€è¦ç´„ã€å½±éŸ¿ã‚’å—ã‘ã‚‹è£½å“ã€è„†å¼±æ€§ã®ã‚ã‚‹è£½å“ãƒªã‚¹ãƒˆã‚’ |
| 1.10 | è„†å¼±æ€§ã‚’å«ã‚“ã§ã„ãªã„ã“ã¨ã‚’ç¢ºèªã•ã‚Œã‚Ÿè£½å“ãªã®ãƒªã‚¹ãƒˆã‚’ |
| 1.9 | è„†å¼±æ€§ã®ã‚ã‚‹è£½å“ãƒªã‚¹ãƒˆã‚’æ›´æ–°ã—ã€ã“ã®è„†å¼±æ€§ã®ã‚ã‚‹ãƒãƒ¼ã‚¸ãƒ§ãƒ³ã‚’ |
| 1.8 | è„†å¼±æ€§ã®ã‚ã‚‹è£½å“ãƒªã‚¹ãƒˆã‚’æ›´æ–°ã—ã€ã“ã®è„†å¼±æ€§ã®ã‚ã‚‹ãƒãƒ¼ã‚¸ãƒ§ãƒ³ã‚’ |
| 1.7 | è„†å¼±æ€§ã®ã‚ã‚‹è£½å“ãƒªã‚¹ãƒˆã‚’æ›´æ–°ã—ã€ã“ã®è„†å¼±æ€§ã®ã‚ã‚‹ãƒãƒ¼ã‚¸ãƒ§ãƒ³ã‚’<br>Under Affected Products added further clarification on products not listed. |
| 1.6 | è„†å¼±æ€§ã®ã‚ã‚‹è£½å“ãƒªã‚¹ãƒˆã‚’æ›´æ–°ã—ã€ã“ã®è„†å¼±æ€§ã®ã‚ã‚‹ãƒãƒ¼ã‚¸ãƒ§ãƒ³ã‚’ |
| 1.5 | è„†å¼±æ€§ã®ã‚ã‚‹è£½å“ãƒªã‚¹ãƒˆã‚’æ›´æ–°ã—ã€ã“ã®è„†å¼±æ€§ã®ã‚ã‚‹ãƒãƒ¼ã‚¸ãƒ§ãƒ³ã‚’ |
| 1.4 | è„†å¼±æ€§ã®ã‚ã‚‹è£½å“ãƒªã‚¹ãƒˆã‚’æ›´æ–°ã—ã€ã“ã®è„†å¼±æ€§ã®ã‚ã‚‹ãƒãƒ¼ã‚¸ãƒ§ãƒ³ã‚’ |

| Version | Descripti |
| --- | --- |
| 1.3 | è„†å¼±æ€§ã•Œå˜åœ¨ã•™ã‚‹è£½å“•ã€•è„†å¼±æ€§ã‚’å•«ã‚“ã•§ã•„ã•ªã•„è£½å“•ã€‹ |
| 1.2 | è„†å¼±æ€§ã•Œå˜åœ¨ã•™ã‚‹è£½å“•ã€•è„†å¼±æ€§ã‚’å•«ã‚“ã•§ã•„ã•ªã•„è£½å“•ã€‹ |
| 1.1 | è„†å¼±æ€§ã•Œå˜åœ¨ã•™ã‚‹è£½å“•ã€•è„†å¼±æ€§ã‚’å•«ã‚“ã•§ã•„ã•ªã•„è£½å“•ã€‹<br>Added the SIR value for each vulnerability. Added information about public exploitation. |
| 1.0 | åˆ•å›žå…¬é–‹ãƒªãƒªãƒ¼ã‚¹ |

## åˆ©ç”¨è¦ç´„

æœ¬ã‚µãƒ¼ãƒ“ã‚¹ã•¯ç„¡ä¿è¨¼ã•®ã•‚ã•®ã•¨ã•—ã•¦æ••ä¾›ã•—ã•¦ã•Šã‚Šã€
æœ¬ã‚µãƒ¼ãƒ“ã‚¹ã•¯ã€•ã‚µãƒ¼ãƒ“ã‚¹ã•®æƒ…å ±ã•Šã‚ˆã•³ã‚µãƒ¼ãƒ“ã‚¯ã•®ä½¿ç”¨ã•«é–¢ã•™ã‚‹è²¬ä»»ã•®ä¸€
ã•¾ã•Ÿã€•ã‚·ã‚¹ãƒ†ãƒ ã•¯æœ¬ã‚µãƒ¼ãƒ“ã‚¹ã•®å†…å®¹ã‚’äº^å‘Šã•ªã•—ã•«å¤‰æ›´ã•—ã•
æœ¬ã‚µãƒ¼ãƒ“ã‚¹ã•®è¨˜è¿°å†…å®¹ã•«é–¢ã•—ã•¦æƒ…å ±é…•ä¿¡ã•® URL
ã‚’çœ•ç•¥ã•—ã€•å•˜ç‹¬ã•®è»¢è¼‰ã„æ„•è¨³ã‚’æ–½ã•—ã•Ÿå ´å•^ã€•å½“ç¤¾ã•Œç®¡ç•
ã•“ã•®ãƒ‰ã‚¤ãƒ¡ãƒ³ãƒˆã•®æƒ…å ±ã•¯ã€•ã‚·ã‚¹è£½å“•ã•®ã‚¨ãƒ³ãƒ‰ãƒ¦ãƒ¼ã‚¶ãƒ¼ã‚’å¯¾è±¡

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。