

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**DATE ISSUED:** September 23, 2009

The following 11 advisories were released by Cisco this week as part of its semi-annual patch release program for IOS products:

- Cisco Security Advisory: Cisco Unified Communications Manager Express Vulnerability  
[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080af8116.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080af8116.shtml)
- Cisco Security Advisory: Cisco IOS Software Internet Key Exchange Resource Exhaustion Vulnerability  
[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080af8117.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080af8117.shtml)
- Cisco Security Advisory: Cisco IOS Software Tunnels Vulnerability  
[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080af8115.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080af8115.shtml)
- Cisco Security Advisory: Cisco IOS Software Object-group Access Control List Bypass Vulnerability  
[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080af8119.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080af8119.shtml)
- Cisco Security Advisory: Cisco Unified Communications Manager Session Initiation Protocol Denial of Service Vulnerability  
[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080af8118.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080af8118.shtml)
- Cisco Security Advisory: Cisco IOS Software H.323 Denial of Service Vulnerability  
[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080af811a.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080af811a.shtml)
- Cisco Security Advisory: Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability  
[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080af811b.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080af811b.shtml)
- Cisco Security Advisory: Cisco IOS Software Crafted Encryption Packet Denial of Service Vulnerability  
[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080af811c.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080af811c.shtml)
- Cisco Security Advisory: Cisco IOS Software Authentication Proxy Vulnerability  
[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080af8132.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080af8132.shtml)
- Cisco Security Advisory: Cisco IOS Software Zone-Based Policy Firewall Vulnerability  
[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080af8130.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080af8130.shtml)
- Cisco Security Advisory: Cisco IOS Software Network Time Protocol Packet Vulnerability  
[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080af8131.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080af8131.shtml)

Additional information can be obtained by visiting:

[http://www.cisco.com/en/US/products/products\\_security\\_advisories\\_listing.html](http://www.cisco.com/en/US/products/products_security_advisories_listing.html)