

25 September 2008

By: Lucian Constantin, Web News Editor



Cisco multiple security
advisories released
Cisco Systems, Inc.

[Cisco Releases Several Important Security Advisories](#)

All of the advisories address significant vulnerabilities in several Cisco products

Cisco [published](#) no less than 12 new security advisories on September 24 describing multiple moderate and high risk vulnerabilities that affect the IOS software and the Cisco Unified Communications Manager. Software updates have been released to address some of these security issues, so updating immediately is highly encouraged.

A [Vulnerability in Cisco IOS While Processing SSL Packet](#) may result in a device crashing when a SSL session is terminated while processing a particular packet. All devices based on the IOS software that are using SSL-based services are affected by this vulnerability. The 12.4 and 12.4MR software releases are reported as being affected and update to 12.4(18c), respectively 12.4(19)MR is recommended.

[Multiple Multicast Vulnerabilities in Cisco IOS Software](#) involving maliciously crafted PIM packets may result in denial of service (DoS). All devices that are configured for PIM and running the IOS Software are vulnerable. A [list](#) of recommended software updates is included.

A [Cisco IOS NAT Skinny Call Control Protocol Vulnerability](#) may cause devices to reload due to a series of segmented SCCP messages. Repeated exploitation can result in denial of service. Devices running the IOS Software with NAT SCCP Fragmentation support are vulnerable. Several 12.4-Based releases are affected and [updates](#) have been issued for all of them.

[Multiple Cisco IOS Session Initiation Protocol Denial of Service Vulnerabilities](#) are remotely exploitable and can cause memory leaks and device reloading. Only IOS devices that have enabled the SIP voice services are affected. A [list](#) with fixed software releases has been published.

[Multiple Cisco Products are Vulnerable to DNS Cache Poisoning Attacks](#). This is due to insufficient randomization of DNS transactions IDs and source ports. Products that can be set up as DNS servers are vulnerable. This includes devices based on Cisco IOS Software, Cisco Network Registrar, Cisco Application and Content Networking System and the Cisco Global Site Selector Used in Combination with Cisco Network Registrar. Software [updates](#) for all affected releases have been published.

[Cisco Unified Communications Manager Session Initiation Protocol Vulnerabilities](#) can result in denial of service by interrupting the voice services. Cisco Unified CallManager and Communications Manager products are affected by these vulnerabilities. Patched software versions that address these vulnerabilities have not been released yet.

A [Cisco uBR10012 Series Devices SNMP Vulnerability](#) can be exploited to gain full access to the device. This is because when configured for linecard redundancy, the devices automatically give SNMP read/write access. Only uBR10012 devices configured as described previously are vulnerable. A [list](#) of patched software version is available.

[Cisco IOS MPLS VPN May Leak Information](#) when devices are "configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding

Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices." Patched [software versions](#) have been released to address the issue.

A [Cisco IOS MPLS Forwarding Infrastructure Denial of Service Vulnerability](#) can be exploited through specially crafted packets. Only Cisco IOS devices that are configured for MPLS and support MFI are affected. A list of software [updates](#) has been released.

A [Cisco 10000, uBR10012, uBR7200 Series Devices IPC Vulnerability](#) can be exploited and result in denial of service because the UDP IPC channel is reachable remotely. Affected versions of the Cisco IOS software have received [updates](#).

A [Cisco IOS Software Firewall Application Inspection Control Vulnerability](#) can result in denial of service upon processing a malformed HTTP packet. Only devices with the HTTP AIC feature enabled are vulnerable. Software [updates](#) have been issued for the affected IOS versions.

A [Cisco IOS Software Layer 2 Tunneling Protocol \(L2TP\) Denial of Service Vulnerability](#) affects a small number of IOS releases. Using a specifically crafted L2TP packet, an attacker could force the device to reload. Updating to the patched software [versions](#) is recommended.