Cisco IOS IPSec IKE Unspecified Denial of Service Vulnerability

Ref ID	NCIT-SB-2012-06	**Vulnerability Identifier**	CISCO
Description	The IKEv1 implementation in Cisco IOS 12.2 through 12.4 and 15.0 through 15.2 and IOS XE 2.1.x through 2.6.x and 3.1.xS through 3.4.xS before 3.4.2S, 3.5.xS before 3.5.1S, and 3.2.xSG before 3.2.2SG allows remote attackers to cause a denial of service (device reload) by sending IKE UDP packets over (1) IPv4 or (2) IPv6, aka Bug ID CSCts38429.		
Impact	Confidentiality **(High)**	Integrity **(High)**	Availability **(High)**
Vulnerability Type	Execute Code, Bypass a restriction or similar		
Release Date	March 29, 2012	**Last Update Date**	April 03, 2012

Summary

Cisco devices that are running Cisco IOS Software are vulnerable when they are configured to use IKE version 1 (IKEv1).
A number of features use IKEv1, including different Virtual Private Networks (VPN) such as:

- LAN-to-LAN VPN
- Remote access VPN (excluding SSLVPN)
- Dynamic Multipoint VPN (DMVPN)
- Group Domain of Interpretation (GDOI)

There are two methods to determine if a device is configured for IKE:

- Determine if IKE ports are open on a running device
- Determine if IKE features are included in the device configuration

Affected Vendors

The vulnerability is reported in version 2.1.x, 2.2.x, 2.3.x, 2.4.x, 2.5.x, 2.6.x, 3.1.x, and 3.3.x.

Solution:

Upgrade to version 3.4.2S.

References

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ike