

# Cisco Security Response: MD5 Hashes May Allow for Certificate Spoofing

<http://www.cisco.com/warp/public/707/cisco-sr-20090115-md5.shtml>

## Revision 1.0

For Public Release 2009 January 15 1600 UTC (GMT)

---

Please provide your [feedback](#) on this document.

---

## Contents

[Cisco Response](#)  
[Status of this Notice: FINAL](#)  
[Revision History](#)  
[Cisco Security Procedures](#)

---

## Cisco Response

This is the Cisco response to research done by Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, and Benne de Weger pertaining to MD5 collisions in certificates issued by vulnerable certificate authorities.

Cisco has released an IntelliShield activity bulletin detailing the specifics of this issue. This bulletin is available at the following link: <http://tools.cisco.com/security/center/viewAlert.x?alertId=17341>.

The Cisco Adaptive Security Appliance (ASA) and IOS may both serve as certificate authorities and by default use the MD5 hashing algorithm in the digital signatures of certificates issued to end users and devices.

The hashing algorithm used in digital certificates on the Cisco ASA cannot be changed; however, the ASA is unlikely to be affected by the attacks described in this research due to the way certificates are generated on the device. Cisco recognizes the weaknesses in MD5 and plans to alter the signature algorithm used in digital certificates and modify the methods utilized in creation of CA and endpoint certificates. This will be addressed by Cisco Bug ID: [CSCsw88068](#) ( [registered](#) customers only) .

The Cisco IOS CA may be vulnerable to the attack described in this research when configured to utilize MD5 hashes in endpoint certificates. This is the default behavior; however, the device can be reconfigured to utilize a more secure hashing algorithm. Cisco plans to change this default behavior and modify the methods utilized in creation of CA and endpoint certificates. This will be addressed

by Cisco Bug ID: [CSCsw90626](#) ( [registered](#) customers only) .

As a workaround, an administrator can configure IOS devices running 12.4(15)T and later to use a more secure algorithm with the **hash** command, as shown in the following example:

```
Router(config)#crypto pki server <NAME>
Router(cs-server)#shutdown
Certificate server 'shut' event has been queued for processing.
Router(cs-server)#hash sha1
Router(cs-server)#no shutdown
Certificate server 'no shut' event has been queued for processing.
```

## Status of this Notice: FINAL

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

## Revision History

Revision 1.0	2009-January-15	Initial public release
--------------	-----------------	------------------------

## Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at [http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html). This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

---

### Help us help you.

-  **Please rate this document.**

- Excellent  
 Good  
 Average  
 Fair  
 Poor

-  **This document solved my problem.**

- Yes
- No
- Just browsing

**Suggestions for improvement:**

(256 character limit)

<a href="#">Home</a>	<a href="#">How to Buy</a>	<a href="#">Login</a>	<a href="#">Profile</a>	<a href="#">Feedback</a>	<a href="#">Site Map</a>	<a href="#">Help</a>
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)