

[Solutions](#) [Products](#) [Ordering](#) [Support](#) [Partners](#) [Training](#) [Corporate](#)[Security Responses](#)

Cisco Security Response: Extensible Authentication Protocol Vulnerability

<http://www.cisco.com/warp/public/707/cisco-sr-20071019-eap.shtml>

Revision 1.5

Last Updated 2007 December 03 0300 UTC (GMT)

For Public Release 2007 October 19 1600 UTC (GMT)

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

Contents

[Cisco Response](#)
[Additional Information](#)
[Revision History](#)
[Cisco Security Procedures](#)

Cisco Response

This is the Cisco PSIRT response to a presentation that was delivered by Laurent Butti, Julien Tinnès and Franck Veysset of France Telecom Group at Hack.lu on October 19th, 2007.

The presentation identifies a vulnerability in Cisco's implementation of Extensible Authentication Protocol (EAP) that exists when processing a crafted EAP Response Identity packet. This vulnerability affects several Cisco products that have support for wired or wireless EAP implementations.


The Cisco PSIRT team greatly appreciates the opportunity to work with researchers on security vulnerabilities, and we welcome the opportunity to review and assist in product reports.

This vulnerability is documented in the following Cisco bug IDs:

- Wireless EAP - [CSCsj56438](#) ([registered](#) customers only)
- Wired EAP - [CSCsb45696](#) ([registered](#) customers only) and [CSCsc55249](#) ([registered](#) customers only)

This Cisco Security Response is available at the following link:
<http://www.cisco.com/warp/public/707/cisco-sr-20071019-eap.shtml>.

Additional Information

As described in [RFC3748](#) , EAP is an authentication framework that supports multiple authentication methods. Typically, EAP runs directly over data link layers, such as Point-to-Point Protocol (PPP) or IEEE 802, without requiring IP.

Vulnerable Products

This vulnerability affects both wired and wireless implementation on Cisco devices.

EAP is not configured by default on any of these Cisco devices.

The following Cisco products support Wireless EAP and are affected by this vulnerability:

- **Access Points and 1310 Wireless Bridges running Cisco IOS in autonomous mode (CSCsj56438).**

Access Points and 1310 Wireless Bridges running in LWAPP mode are not affected. To confirm if an Access Point runs Cisco IOS in autonomous mode, log into the device and issue the command line interface (CLI) command `show version | include IOS`. Access Points in autonomous mode will have `-K9W7-` in the image names, while Access Points in LWAPP mode will have `-K9W8-` in their name. The example below shows an Access Point in autonomous mode:

```
AP#show version | include IOS
Cisco IOS Software, C1240 Software (C1240-K9W7-M), Version 12.4(3g)JA, REL
AP#
```

To determine if EAP is enabled on the Access Point, log into the device and issue the **show running-config** CLI command. If the output contains the **authentication open eap *method_name*** or **authentication network-eap *method_name*** then the device is vulnerable. The example below shows a vulnerable Access Point:

```
AP#show running-config
...
dot11 ssid test
 authentication open eap eap_methods
 authentication network-eap eap_methods
 authentication key-management wpa
 guest-mode
 infrastructure-ssid optional
...
AP#
```

If an attacker successfully exploits this vulnerability against an Access Point, the device will reload. Repeated exploitation will result in a sustained Denial of Service (DoS) attack. This vulnerability was reported to Cisco by Laurent Butti and Benoît Stopin.

- **Cisco Catalyst 6500 Series Switch and Cisco 7600 Series Wireless LAN Services Module**

(CSCsj56438)

To determine if EAP is enabled on the Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM), log into the WLSM and issue the "**show running-config**" CLI command. If the output contains "wlccp authentication-server client <any | eap | leap> <list_name>" and/or "wlccp authentication-server infrastructure <list>" then the device is vulnerable. The example below shows a vulnerable WLSM:

```
WLAN#show running-config
...
aaa group server radius rad_eap
server 10.22.222.2 auth-port 1812 acct-port 1813
!
aaa authentication login eap_list group rad_eap
...
...
wlccp authentication-server infrastructure eap_list
wlccp authentication-server client any eap_list
...
WLAN#
```

If an attacker successfully exploits this vulnerability against a WLSM, the module will reload. Repeated exploitation will result in a sustained Denial of Service (DoS) attack.

The following Cisco products support Wired EAP and are affected by this vulnerability.

- **All Cisco switches running affected versions of Cisco IOS (CSCsb45696).**

Cisco switches are vulnerable if they run an EAP authenticator. EAP supplicants are not vulnerable.

To determine if EAP authenticator is enabled on a switch, log into the device and issue the **show running-config | include dot1x** CLI command. If the output contains either **dot1x pae authenticator** or **dot1x pae both**, then the device is vulnerable to exploits via the interface where these commands appear. The example below shows a device that has EAP authenticator enabled:

```
switch#show running-config | include dot1x
dot1x system-auth-control
dot1x pae authenticator
dot1x port-control auto
dot1x timeout quiet-period 1
dot1x timeout ratelimit-period 1
dot1x max-start 10
dot1x max-req 10
switch#
```

A related Cisco bug ID, [CSCsi70426](#) ([registered](#) customers only), exists and displays a traceback message on the console or syslogs when receiving the crafted EAP-ID-RESPONSE packet. However, the device will continue to operate.

- **All Cisco switches running affected versions of Cisco CatOS (CSCsc55249).**

The Cisco switches are vulnerable if running an EAP authenticator. EAP supplicants are not vulnerable.

To determine if EAP authenticator is enabled on a switch, log into the device and issue the **show run all | include dot1x** CLI command. If the output contains both **set dot1x system-auth-control enable** and any occurrence of **set port dot1x <mod/port> port-control auto**, then the device is vulnerable for exploitation via the port where the **set port dot1x** commands appear. An example

is shown below of a device that has EAP authenticator enabled:

```
Console> (enable) show run all | include dot1x
#dot1x
set dot1x system-auth-control enable
set dot1x quiet-period 60
set dot1x tx-period 30
set dot1x shutdown-timeout 300
set dot1x supp-timeout 30
set dot1x server-timeout 30
set dot1x max-req 2
set dot1x max-reauth-req 2
set dot1x re-authperiod 3600
set dot1x radius-accounting disable
set dot1x radius-vlan-assignment enable
set dot1x radius-keepalive enable
set dot1x critical-recovery-delay 100
set port dot1x 10/2 port-control auto
Console> (enable)
```

- **Cisco Unified Communications 500 Series**

The 8- and 16-user models of the Cisco Unified Communications 500 (UC500) Series support an optional integrated WLAN access point for secure WLAN connectivity. If the UC500 has the optional WLAN access point installed and configured, the UC500 is affected by this vulnerability. To determine if the optional integrated WLAN access point is installed in the UC500, log into the device and enter the CLI command "show version | include Radio". Shown below is the output of a device with an optional WLAN access point installed. A device without the WLAN access point installed will output no data from the entered command.

```
UC500#show version | include Radio
      1 802.11 Radio
UC500#
```

To confirm if the UC500 is running affected configuration if the optional integrated WLAN access point is installed, refer to the details within the "Access Points and 1310 Wireless Bridge running Cisco IOS in autonomous mode" section above.

There are no workarounds for this vulnerability on wired or wireless implementations of EAP.

Successful exploitation of the vulnerability on either the wired or wireless device will result in a reload of the device. Repeated exploitation could result in a sustained DoS attack.

The list below describes the affected trains and the first fixed release:

Wireless EAP - CSCsj56438	
Affected Release	First Fixed Releases
12.3.JA	Vulnerable; For AP1100s & AP1200s migrate to 12.3(8)JEC or later.

	For AP1130, AP1240, AP1310 & AP1410 migrate 12.4(10b)JA or later.
12.3.JEA	Vulnerable; migrate to 12.3(8)JEC or later
12.3.JEB	Vulnerable; migrate to 12.3(8)JEC or later
12.3.JEC	12.3(8)JEC or later
12.4.JA	12.4(10b)JA or later
12.4.JX	Vulnerable; migrate to 12.4(10b)JA or later
12.4.XW	12.4.XW5 or later
WLSM (All releases)	2.3.2 or later
Wired EAP (Cisco IOS) - CSCsb45696	
Affected Major Release	First Fixed Releases
12.1	12.1(27b)E2 or later
	12.1(22)EA6 or later
	12.1(26)EB2 or later
12.2	12.2(18)EW6 or later
	12.2(18)S13 or later
	12.2(18)SXF9 or later
	12.2.18-ZY1 or later
	12.2(20)S13 or later
	12.2(25)EWA4 or later
	12.2(25)EX or later
	12.2(25)FX or later
	12.2(25)SED or later
	12.2(25)SG or later
	12.2(31)SB6 or later
12.2(33)SRA4 or later	
Wired EAP (Cisco CatOS) - CSCsc55249	
Affected Major Release	First Fixed Releases
6.x	Vulnerable; migrate to 7.x or 8.x
7.x	7.6(23) or later

8.x	8.5(9) or later
	8.6(1) or later

No other Cisco IOS major release trains are known to be affected by this vulnerability.

For more information on the terms "releases" and "trains," consult the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a008018305e.sht

Products Confirmed Not Vulnerable

The following Cisco products that support the EAP framework have been confirmed as not affected by this vulnerability:

- Access Points
 - Access Points running VxWorks (Cisco 1000s)
 - Lightweight Access Point (LAP) in local mode
 - Lightweight Access Point (LAP) in H-/REAP mode
 - 1310 Wireless Bridge operating in LWAPP mode
 - 1410 Wireless Bridge.
- Wireless LAN Controllers
 - Cisco Airespace 3500 Series WLAN Controller
 - Cisco Airespace 4000 Series Wireless LAN Controller
 - Cisco 2000 series wireless LAN controllers
 - Cisco 2100 Series Wireless LAN Controllers
 - Cisco 4100 Series Wireless LAN Controllers
 - Cisco 4400 Series Wireless LAN Controllers
 - Cisco Wireless LAN Controller Module (NM-AIR-WLC6-K9)
 - Cisco Catalyst 3750 Series Integrated WLC
 - Cisco Catalyst 6500 Series WiSM
- Wireless Integrated Routers (Wireless Access Point - Wireless EAP and Wired EAP)
 - Cisco 800 Series Routers
 - Cisco 1800 Series Integrated Services Routers
 - Cisco 2800 Series Integrated Services Routers
 - Cisco 3200 Series Wireless and Mobile Routers
 - Cisco 3800 Series Integrated Services Routers
- Mobile Wireless
 - Cisco 526 Wireless Express Mobility Controller

THIS SECURITY NOTICE 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 Security Notice 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 1.5	2007-December-03	Updated Wireless EAP software table with information for WLSM and Cisco IOS Software Release 12.4.XW. Added Cisco Unified Communications 500 Series under Vulnerable Products section.
Revision 1.4	2007-October-30	Revised product heading and added a new product line under Vulnerable Products section. Added WLSM to the Wireless EAP table.
Revision 1.3	2007-October-30	Updated software tables for Wireless EAP and Wireless EAP (CatOS).
Revision 1.2	2007-October-29	Updated software tables for Wireless EAP and Wireless EAP (CatOS).
Revision 1.1	2007-October-26	Updated software tables for Wireless EAP and Wireless EAP (CatOS); Removed Cisco 521 Wireless Express Access Point from Products Confirmed Not Vulnerable.
Revision 1.0	2007-October-19	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. 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)

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

All contents are Copyright © 2006-2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).