

Table of Contents

<u>Cisco Security Notice: Response to BugTraq – Cisco ACL Bug when using VPN Crypto Engine Accelerator, PPPoE Dialer or IP Route–Cache</u>	1
<u>Revision 1.0</u>	1
<u>Last Updated 2003 May 15</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Details</u>	1
<u>Cisco Security Procedures</u>	3

Cisco Security Notice: Response to BugTraq – Cisco ACL Bug when using VPN Crypto Engine Accelerator, PPPoE Dialer or IP Route–Cache

Revision 1.0

Last Updated 2003 May 15

Please provide your feedback on this document.

Summary
Details
Cisco Security Procedures

Summary

This document is provided to simplify access to Cisco responses to possible product security vulnerability issues posted in public forums for Cisco customers. This does not imply that Cisco perceives each of these issues as an actual product security vulnerability. This notice is provided on an "as is" basis and does not imply any kind of guarantee or warranty. Your use of the information on the page or materials linked from this page are at your own risk. Cisco reserves the right to change or update this page without notice at any time.

Details

Original Report: <http://www.securityfocus.com/archive/1/321552/2003-05-12/2003-05-18/0> . Cisco responded with the following, which is also archived at <http://www.securityfocus.com/archive/1/321616/2003-05-12/2003-05-18/0> .

```
To: BugTraq
Subject: Re: Cisco ACL bug when using VPN crypto engine accelerator, PPPoE dialer or ip ro
Date: May 15 2003 4:56PM
Author: Ilker Temir <itemir@cisco.com>
Message-ID: <Pine.GSO.4.53.0305151853370.1898@bru-cse-128.cisco.com>
In-Reply-To: <20030514145244.9817.qmail@www.securityfocus.com>
```

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
```

```
This is in response to the e-mail sent by Olivier. The original e-mail is
available at
http://www.securityfocus.com/archive/1/321552/2003-05-12/2003-05-18/0
```

```
Hi Olivier,
```

```
We can confirm that the inbound ACL is processed twice for IPSec traffic
which is the root cause of the issue you have described.
```

```
This issue is being addressed by the Cisco Bug ID CSCdz54626. Cisco's
Product Security Incident Response Team (PSIRT) was not previously aware
of it. We are now addressing it with due priority.
```

While this issue does cause administrative overhead to configuration, there is no significant security impact.

Permitting internal networks in the inbound ACL may be exploited to inject spoofed packets into the network. However this has no practical impact while using static crypto maps. With static crypto maps, the unencrypted traffic will be dropped even if it passes the inbound ACL.

In the case of dynamic crypto maps, in order to bypass the inbound ACL to inject spoofed packets, an attacker would also require control of the neighboring routers that are connected to the interface where the inbound ACL is applied, or the medium in between the neighbors.

Protecting our customers' networks is very important for us and we are always open for vulnerability reports regarding any Cisco product. Such reports should be directly sent to psirt cisco com or security-alert cisco com

Thank you again for your report,

Regards,

- - -

Ilker Temir
Incident Manager, PSIRT
Cisco Systems, Inc.
+32 2 704-6031
<http://www.cisco.com/go/psirt>

On Wed, 14 May 2003, Olivier wrote:

```
>
>
> Platform Cisco 1760 dual Ethernet
>
> IOS 12.2.xT IP/ADSL/FW/IDS PLUS IPSEC 3DES
>
> Environment: Site to site VPN for small offices.
>
>
>
> ACL are not properly parsed as soon as you enable:
>
> crypto engine accelerator
> PPPoE dialer
> Ip route-cache
>
>
> Without the feature mentioned above, you can apply an ACL on the outside
> interface allowing only inbound ISAKMP and IPSEC traffic.
>
> I.E.
>
> ip access-list extended Block-Inbound-unwanted-Traffic
>
> permit udp 100.100.100.0 0.0.0.255 host 102.168.1.2 eq isakmp
>
> permit esp 100.100. 100.0 0.0.0.255 host 102.168.1.2
>
> deny ip any any log
>
>
>
```

```

> If you activate the crypto engine, the ACL is parsed as well on decrypted
> traffic which forces you to allow as well all traffic for the decrypted
> traffic.
> I.E. If you are using 10.x addressees internally and the subnet
> 10.200.0.0/24 for your Soho LAN. Can be worst if you have a huge network
> inside where you would prefer to add permit ip any 10.200.0.0 0.0.0.255.
>
>
> ip access-list extended Block-Inbound-unwanted-Traffic
> permit udp 100.100.100.0 0.0.0.255 host 102.168.1.2 eq isakmp
> permit esp 100.100. 100.0 0.0.0.255 host 102.168.1.2
> permit ip 10.0.0.0 0.255.255.255 10.200.0.0 0.0.0.255 <-----@%#$$%@
> deny ip any any log
>
>
> This looks pretty bad for a VPN box running a Firewall feature set IOS
> seen as the best candidate for VPN for small offices.
>
> The worst is the reply from Cisco:
> -----
> We will be addressing this in the next few months however
> the release time frame could be as late as the end
> of the year.
>
> We do have plans to address it but do
> not expect it in a released image until the
> last calendar quarter of the year. If its possible we
> can get it done and released sooner than what I've
> mentioned, we will do it, no guarantees however.
> -----
>
> We would have hope that they put more resources and concern in solving
> security issue.
>
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.1 (SunOS)

iD8DBQE+w8bR8/wE0ppYtwURAunzAJ4oUlepUBjdJzQ1jzfbQGNI3UNNkwCcCcrh
CJBxZPAMkMO9/PwFxFcibTs=
=4dJU
-----END PGP SIGNATURE-----

```

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/warp/public/707/sec_incident_response.shtml. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.