

Alteon ACEdirector signature/security bug

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-01/0328.html>

From: Dave Plonka (plonka@doit.wisc.edu)

Date: 01/25/02

Date: Fri, 25 Jan 2002 16:09:40 -0600
From: Dave Plonka <plonka@doit.wisc.edu>
To: bugtraq@securityfocus.com

This is to inform you of a bug in the Nortel Alteon ACEdirector product. In some circumstances, this bug raises a security issue since HTTP clients could exploit it to determine the IP addresses of ostensibly "hidden" web servers that are load-balanced by the ACEdirector. In more circumstances, this bug also enables someone to determine whether or not a given Internet web service utilizes ACEdirector equipment by remotely probing that service's IP address.

BACKGROUND

The Nortel/Alteon ACEdirector product ("<http://www.nortelnetworks.com/products/01/acedir/>") has a feature called "Server Load Balancing" (SLB). This feature can be used to load balance incoming HTTP requests made to one virtual IP (vip) address amongst the real IP (rip) addresses of multiple HTTP servers. When enabling an additional feature called "Cookie-Based Persistence", the ACEdirector observes the value of a specific HTTP cookie (when it is present in client request packets) and uses it to persistently map a series of HTTP client requests to the the same one of the real HTTP servers amongst which it is load balancing. This results in the benefit of the the same client to be directed to the same server as long as the client keeps supplying the same cookie value. This persistence is advantagous and sometimes necessary for particular web-based applications that cache client session information on the web server.

PROBLEM

While running Alteon WebOS 9.0 software, a couple of problems have been identified when an ACEdirector is performing server load balancing with cookie-based persistence enabled. (An example of such a configuration is included below.) These problems are:

- 1) The ACEdirector mishandles TCP streams from HTTP clients that make use of the TCP `half-close' feature. This errant behavior could be

SecurityFocus Bugtraq: Alteon ACEdirector signature/security bug

used as a signature to identify ACEdirector equipment on the Internet. It is possible for an HTTP client to craft an HTTP request which will elicit erroneous behavior: either (a) the HTTP session will terminate with no information being returned to client or (b) the client's session will block indefinitely. See W. Richard Stevens `TCP/IP Illustrated Volume 1 for a complete discussion of the TCP half-close feature.

Current versions of commercial browsers such as Netscape and Internet Explorer do not appear to utilize TCP's half-close feature, so users of these applications are unlikely to experience the direct effects of this problem. However, if elicited by an unusual web client application such as nc (a.k.a. "netcat"), a web "spider", or a custom perl script, this erroneous behavior essentially discloses to the client that the web service may be load-balanced by the ACEdirector product. See the perl script below, named "acedirector_request", for an example of how to elicit this erroneous behavior.

- 2) Furthermore, by crafting and sending a peculiar HTTP request to the ACEdirector's virtual IP address (vip), it is sometimes possible for an HTTP client to discover the real IP address(es) of the "hidden" HTTP server(s). During experimentation, it has been observed that it is possible to cause the ACEdirector to erroneously forwards packets back to that client directly from those "hidden" HTTP server(s). (Normally, in a configuration such as that shown below, the ACEdirector would rewrite the source IP address and port number of the packet before forwarding it back to the HTTP client, thereby keeping the HTTP server(s) real identity hidden.)

This is a potential security issue since one can theoretically determine the IP addresses of the hidden servers that are part of a load-balanced system, possibly opening them up to direct attack from malicious parties unless additional firewalling policies are employed. The "acedirector_request" perl script below, when invoked with the "-c" (cookie) option is one example of how to elicit the erroneous behavior described. If an appropriate cookie name or name prefix is specified for the web service in question (e.g. often "ASPSESSIONID" for Microsoft web server applications) the client running this script will often receive a portion of the HTTP response as unexpected packets from one of the HTTP servers real IP addresses. The client host's TCP implementation will usually respond with a TCP RST (ReSeT) packet to each of these unexpected packets because these packets headers contain a source IP address and TCP port numbers that were previously known only to the Alteon ACEdirector.

To put it another way, the ACEdirector will sometimes "leak" packets from a hidden web server's real IP address to a client which had previously established a connection to the ACEdirector's virtual IP address but has since been "half-closed" by the client. Presumably

SecurityFocus Bugtraq: Alteon ACEdirector signature/security bug

this leak occurs because the ACEdirector erroneously flushes an HTTP connection's state information nearly immediately after the half-close occurs, disrupting the web servers session. After it has "forgotten" that session, it subsequently behaves as a normal ethernet switch by simply forwarding subsequent packets to the client without rewriting the IP address and port number of the packet headers.

SOLUTION

No solution has been determined at this time. This problem was reported to Nortel and we prepared traces showing the errant behavior. This resulted in Nortel Networks Case Number 011211-76677 which was opened December 11, 2001.

As of January 25, 2002, we had not received any case update, so we visited Nortel's online tracking system which shows that the case has been `_closed_` with these notes:

This is not considered to be a high priority bug as most browsers that would be affected by half open connection states do not send cookie requests in this manner [...]

Not Applicable to any real world scenario.

WORKAROUND

When using the ACEdirector in the configuration described, it is insufficient to merely configure server load balancing on an ACEdirector to safely hide the identity of the HTTP servers from the clients.

If you don't wish HTTP clients to be able to discover the real IP addresses of the "hidden" HTTP servers (so that they could attempt to interact with those servers directly), one workaround is to introduce a firewall between the clients and the ACEdirector which prevents HTTP clients from sending or receiving packets directly to or from the IP addresses of the real HTTP servers.

EXAMPLE CONFIGURATION

The following is a sample of the portions of the ACEdirector configuration that are relevant to the problems described above:

```
# Enable Server Load Balancing:
```

```
  /c/slb  
    on
```

```
# Define one or more "real" servers:
```

SecurityFocus Bugtraq: Alteon ACEdirector signature/security bug

```
/c/slb/real 20
  ena
  rip 10.42.69.10
/c/slb/real 21
  ena
  rip 10.42.69.11
```

Define a group of "real" servers:

```
/c/slb/group 20
  metric roundrobin
  health http
  add 20
  add 21
```

Define a "virtual" server:

```
/c/slb/virt 20
  ena
  vip 10.69.42.10
```

Configure the virtual server so that it will load balance the HTTP
service, and enable cookie-based persistence:

```
/c/slb/virt 20/service http
  group 20
  dbind ena
/c/slb/virt 20/service 80/pbind cookie passive ASPSESSIONID* 1 24 disable
/c/slb/virt 20/service 80/rcount 10
```

ATTACHED SCRIPT: "acedirector_request"

```
usage: acedirector_request [-c COOKIE] web_server
```

When used on a "real" web server, should return the results of a "GET /".

When used on an ACEdirector, it will report:

```
web_server did not response to TCP half-closed request.
It might be an ACEdirector.
```

If you use the "-c COOKIE" option it will report "leaked" packets, e.g. "-c ASPSESSIONID" for an ACEdirector configured as shown above. This method by which this script shows leaked packets is a total kludge in that it launches tcpdump(1). At that time, hit CTRL-C to break out of it after a reasonable amount of time. (If one wanted to automate this exploit, using Net::RawIP with a timeout might be preferable.)

DISCLAIMER

SecurityFocus Bugtraq: Alteon ACEdirector signature/security bug

Use the "acedirector_request" script to test your web servers or ACEdirector equipment at your own risk. AFAIK, the script is totally innocuous when testing an HTTP server that allows TCP half-close such as IIS or Apache – it simply performs a "GET /". When testing an ACEdirector, it appears not to cause any harm and simply elicits the erroneous behavior.

--
plonka@doit.wisc.edu <http://net.doit.wisc.edu/~plonka> ARS:N9HZF Madison, WI

- text/plain attachment: [acedirector_request](#)
-

- *Previous message:* bugzilla@redhat.com: "[RHSA-2002:018-05] New rsync packages available"
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)