

[NEWS] Pyramid BenHur Firewall Active FTP Portfilter Ruleset Results in a Firewall Leak

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0088.html>

From: support@securiteam.com

Date: 07/22/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 22 Jul 2002 18:10:33 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> - Know that you're safe.

Pyramid BenHur Firewall Active FTP Portfilter Ruleset Results in a Firewall Leak

SUMMARY

A security vulnerability in <<http://www.pyramid.de/>> Pyramid's BenHur Firewall allows attackers to connect and scan internally protected ports by assigning their scanning port to port number 20 (the port used by FTP's data connection).

DETAILS

Vulnerable systems:

- * BenHur Firewall release 3 update 066 fix 2

Immune systems:

- * BenHur Firewall release 3 update 067 (experimental)

Source port 20 on a client's side of the communication can be used to connect to services on ports between 1024 and 65096 on release "Update 066 fix 2", and on ports between 1024 and 65535 on the product's initial installed release.

Securiteam: [NEWS] Pyramid BenHur Firewall Active FTP Portfilter Ruleset Results in a Firewall Leak

Technical details:

One can connect to the ports using e.g. netcat: "nc -p 20 \$benhur \$remoteport"

This makes it possible to connect to several active TCP ports on BenHur:

tcp 0 0 0.0.0.0:3128 0.0.0.0:* LISTEN -> Squid protected by Squid-ACL against misuse from outside

tcp 0 0 0.0.0.0:8888 0.0.0.0:* LISTEN -> BenHur Web administration not protected by IPv4-ACL, see below

tcp 0 0 0.0.0.0:4557 0.0.0.0:* LISTEN -> HylaFAX client server (possible access not tested)

tcp 0 0 0.0.0.0:4559 0.0.0.0:* LISTEN -> HylaFAX client server (possible access not tested)

tcp 0 0 0.0.0.0:6105 0.0.0.0:* LISTEN -> ISDN client server monitor and connection trigger program (possible access not tested)

Especially the BenHur Web administration port is interesting:

```
# nc -p 20 ***.***.***.*** 8888
GET / HTTP/1.0
```

HTTP/1.1 401 Authorization Required

Date: Tue, 09 Jul 2002 09:53:51 GMT

Server: Apache/1.3.0 (Unix) Debian/GNU

WWW-Authenticate: Basic realm="Ben-Hur Administration"

Connection: close

Content-Type: text/html

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
```

```
<HTML><HEAD>
```

```
<TITLE>401 Authorization Required</TITLE>
```

```
</HEAD><BODY>
```

```
<H1>Authorization Required</H1>
```

This server could not verify that you are authorized to access the document you requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.<P>

```
</BODY></HTML>
```

Background on FTP and stateless packet filters:

As known, ipchains is (in contrast to iptables of 2.4.x) a stateless packet filter and is only able to make decisions based on the data of a single packet (e.g. Source IP, or the status of the TCP-specific SYN flag).

A good firewall ruleset built for a stateless packet filter is more complicated than the equivalent ruleset for a stateful packet filter. Especially the rules controlling active FTP (client inside, server outside) is among the most prominent reasons for security holes in a firewall configuration.

Securiteam: [NEWS] Pyramid BenHur Firewall Active FTP Portfilter Ruleset Results in a Firewall Leak

If a firewall allows active FTP from the inside to the outside, the administrator has to allow everyone outside to establish a TCP session from source port 20 to a port on or beyond the firewall numbered 1024 or above. This port is specified either by the FTP client directly (after asking the local system for a free port), or by the masquerading engine (if FTP client is on an internal network behind the firewall, not on the firewall itself).

Both port ranges are known:

- A) See `/proc/sys/net/ipv4/ip_local_port_range`, which is normally 1024–4999 (see also `net/ipv4/tcp_ipv4.c`)
- B) 61000–65095 (see kernel sources `ip_masq.[hc]`)

Problems in the BenHur configuration:

There are more than one reason why BenHur is vulnerable:

- 1) BenHur is currently using the following dangerous ruleset for active FTP:

```
chain: input
ACCEPT tcp ----- 0xFF 0x00 ppp0 0.0.0.0/0 0.0.0.0/0 20 -> 1024:65096
```

Therefore, any incoming TCP connection requests to ports between 1024 and 65096 are permitted.

This rule is set by script `/etc/init.d/ben-hur.ipchains` in following lines:

```
$IPCHAINS -A input --source-port 20 -d $WORLD 1024:65096 -p tcp \
-i $IFACE_WWW -j ACCEPT
```

```
$IPCHAINS -A output --source-port 20 -d $HOME 1024:65096 -p tcp \
-i $IFACE_LAN -j ACCEPT
```

- 2) All daemons listening on ports ≥ 1024 bind to IPv4 "any" and not e.g. to internal IPv4 address only.

- 3) Not all daemons have an ACL that denies a request from outside on higher level, e.g. using `tcp_wrappers` or a built-in ACL system (c.f. Squid).

How to prevent this vulnerability:

There are several solutions to close such holes in general:

- 1) For masqueraded active FTP connection, the destination port on the firewall is always mapped to a port in the range 61000–65095 by the module "ip_masq_ftp". Therefore a rule like

```
chain: input
ACCEPT tcp ----- 0xFF 0x00 ppp0 0.0.0.0/0 0.0.0.0/0 20 -> 61000:65095
```

Securiteam: [NEWS] Pyramid BenHur Firewall Active FTP Portfilter Ruleset Results in a Firewall Leak

Would be more appropriate. The above translates to the following lines replacing the corresponding lines in the /etc/init.d/ben-hur.ipchains in script quoted above:

```
$IPCHAINS -A input --source-port 20 -d $WORLD 61000:65095 -p tcp \  
-i $IFACE_WWW -j ACCEPT
```

```
$IPCHAINS -A output --source-port 20 -d $HOME 1024:65535 -p tcp \  
-i $IFACE_LAN -j ACCEPT
```

Note: In the original setup, the script contains a (not security related) bug in the port range for the output chain on the internal interface. This improvement is also done in BenHur software update 067.

2) If the firewall itself uses active FTP, then the local port range should be generally moved to a less dangerous region, e.g. 32768-60999 by using:

```
sysctl -w net.ipv4.ip_local_port_range="32768 60999"
```

Or equivalently:

```
echo "32768 60999" >/proc/sys/net/ipv4/ip_local_port_range
```

You are advised to ensure that the range used for ip_local_port_range does not conflict with any LISTENING ports on the firewall itself. If not able to move the local port range for now, you should at least reduce the impact by a second more selective rule for the input chain:

```
LOCALPORTRANGE=""`cat /proc/sys/net/ipv4/ip_local_port_range | awk '{ print  
$1 ":" $2 }`""  
$IPCHAINS -A input --source-port 20 -d $WORLD $LOCALPORTRANGE -p tcp \  
-i $IFACE_WWW -j ACCEPT
```

Normally this results in following ruleset

chain: input

```
ACCEPT tcp ----- 0xFF 0x00ppp0 0.0.0.0/00.0.0.0/0 20 -> 1024:4999
```

3) Restrict the LISTENING socket bindings of the daemons as much as possible (making them listen only on the local interface and thus making connections from the outside impossible), and/or employ an ACL system:

- * Daemon-built-in-ACLs
- * tcp_wrapper (if possible)
- * Creating dedicated block rules for active server ports >= 1024

Vendor response:

09 Jul 2002: E-mail to <support.solutions (at) pyramid.de> and <support (at) pyramid.de>
10 Jul 2002: Human response via e-mail by Lars Degenhardt <lars.degenhardt (at) pyramid.de>

19 Jul 2002: Received information that experimental update 067 fixes this issue

ADDITIONAL INFORMATION

Securiteam: [NEWS] Pyramid BenHur Firewall Active FTP Portfilter Ruleset Results in a Firewall Leak

The information has been provided by <mailto:pbieringer@erasesec.de> Dr. Peter Bieringer.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- **Previous message:** support@securiteam.com: "[NEWS] PHP Security Vulnerability in Multipart FORM Data Handling"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)