

# [NEWS] Raptor Firewall Weak ISN Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0012.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 08/05/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Mon, 5 Aug 2002 17:35:02 +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.

-----

Raptor Firewall Weak ISN Vulnerability

---

## SUMMARY

Raptor Firewall is Symantec's implementation of a firewalling/proxy application. A problem exists within the IP stack implementation of Raptor Firewall during the generation of the Initial Sequence Numbers ("ISNs"). The algorithm used for generating these ISNs is not sufficiently random and could allow a remote attacker to hijack any connection to or traversing the Raptor Firewall.

## DETAILS

Vulnerable systems:

- \* Raptor Firewall 6.5 (Windows NT)
- \* Raptor Firewall V6.5.3 (Solaris)
- \* Symantec Enterprise Firewall 6.5.2 (Windows 2000 and NT)
- \* Symantec Enterprise Firewall V7.0 (Solaris)
- \* Symantec Enterprise Firewall 7.0 (Windows 2000 and NT)
- \* VelociRaptor Model 500/700/1000
- \* VelociRaptor Model 1100/1200/1300
- \* Symantec Gateway Security 5110/5200/5300

During the transport and forwarding of packets, Initial Sequence Numbers ("ISNs") are generated by the Raptor Firewall's IP stack. A weakness in the generation of these ISNs could allow a remote attacker to easily

## Securiteam: [NEWS] Raptor Firewall Weak ISN Vulnerability

predict the sequence numbers for a certain session.

The generation of the ISNs is based on two factors: the source and destination port, and the source and destination IP. For a single connection, an initial sequence number will not change for a certain [long] amount of time. An example connection ("session") can be described as follows:

```
session = {[src ip:src port] [dst ip:dst port]}
```

An ISN is attributed to a specific sessions for a certain amount of time. Below are some excerpts of real-life tests performed against a Raptor Firewall. The following tests sends SYN packets from a source address [x.x.x.x] on a source-port [1700] to a destination address [z.z.z.z] on a destination port [80] over a period of several minutes.

---

### Timeline Connection ISN Delta

---

```
10:33:05 x.x.x.x:1700 -> z.z.z.z:80 2088144436 -
10:33:06 x.x.x.x:1700 -> z.z.z.z:80 2088144436 0
10:33:07 x.x.x.x:1700 -> z.z.z.z:80 2088144436 0
..
10:35:30 x.x.x.x:1700 -> z.z.z.z:80 2088144436 0
10:35:31 x.x.x.x:1700 -> z.z.z.z:80 2088144436 0
10:35:32 x.x.x.x:1700 -> z.z.z.z:80 2088144436 0
..
10:50:43 x.x.x.x:1700 -> z.z.z.z:80 2088144436 0
10:50:44 x.x.x.x:1700 -> z.z.z.z:80 2088144436 0
10:50:45 x.x.x.x:1700 -> z.z.z.z:80 2088144436 0
```

As shown above, this test clearly shows that the Initial Sequence Number does not change for a significant amount of time. Another test showed that when an ISN is assigned to a session, this session and ISN are stored for future use for a certain amount of time, regardless whether or not several new sessions are established from the same source IP.

This issue has been reproduced against six Raptor Firewalls, each belonging to different administrative bodies.

#### Characteristics:

- \* The ISN for each session is different, but for a single session, the ISN does not change for a considerable amount of time.
- \* This could possibly allow an attacker to hijack the session.
- \* This issue affects all vulnerabilities handled by the Raptor IP stack, including all sessions to and traversing the Raptor Firewall.

#### Severity:

This vulnerability can allow a remote attacker to potentially hijack an

Securiteam: [NEWS] Raptor Firewall Weak ISN Vulnerability

existing connection to or traversing the Raptor Firewall.

Vendor status:

Symantec's Security Response Team ([symsecurity@symantec.com](mailto:symsecurity@symantec.com)) was contacted about this issue on Wednesday, July 03 2002. A coordinated effort between Symantec and Ubizen has lead to quick resolution of this issue. HotFixes are available to eradicate this vulnerability.

Solution:

Symantec has released HotFixes to resolve this issue. They can be found at the following locations:

Technical Bulletin:

<<http://www.symantec.com/techsupp/bulletin/archive/firewall/082002firewall.html>>  
<http://www.symantec.com/techsupp/bulletin/archive/firewall/082002firewall.html>

Patches and HotFixes:

<<http://www.symantec.com/techsupp/>> <http://www.symantec.com/techsupp/>

ADDITIONAL INFORMATION

The information has been provided by  
<<mailto:kristof.philipsen@ubizen.com>> Kristof Philipsen.

=====

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](mailto:list-unsubscribe@securiteam.com)  
In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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](mailto:support@securiteam.com): "[NEWS] Multiple Cyan Chat Vulnerabilites"
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)