

Securiteam: [NEWS] Symantec Enterprise Firewall FTP Bounce Vulnerability (Patch Available)

[NEWS] Symantec Enterprise Firewall FTP Bounce Vulnerability (Patch Available)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-04/0077.html>

From: support@securiteam.com

Date: 04/18/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 18 Apr 2002 21:56:02 +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.

Symantec Enterprise Firewall FTP Bounce Vulnerability (Patch Available)

SUMMARY

Symantec is aware of an FTP Bounce Vulnerability condition reported in our previous post: <http://www.securiteam.com/securitynews/5WP0F206WS.html> Raptor Firewall FTP Bounce Vulnerability. This potential vulnerability could affect some Symantec Enterprise Firewall deployments. Using this FTP-protocol based vulnerability, an attacker could potentially hide an attack by using the firewall identity against an unsuspecting and unprotected external machine. In addition, by overwriting the PORT command with its own internal address, the firewall overwrites the FTP-server built-in protection mechanism that protects against this type of attack.

DETAILS

Affected Versions:

- * Raptor Firewall V6.5.3 (Solaris)
- * Symantec Enterprise Firewall V7.0 (Solaris)

Recommendation:

If the FTP Bounce Attack affects your deployment, please make sure you apply the related Hotfix available from the Symantec Enterprise Support site. This Hotfix is an enhanced version of our FTPd module for the

Securiteam: [NEWS] Symantec Enterprise Firewall FTP Bounce Vulnerability (Patch Available)

affected platforms that extends the protection currently provided by the firewall. Symantec is currently investigating if this problem affects our remaining supported products and platforms and we will release enhanced versions of the FTPd module as necessary.

This module update is available for download from the Symantec Enterprise Support site (<<http://www.symantec.com/techsupp>> <http://www.symantec.com/techsupp>). The following enhancements have been made to the FTPd module for Solaris:

1) By default, if the firewall detects a PORT request destined for an IP address other than the IP address of the FTP client, it will log the following warning:

```
"353 Warning: PORT command referenced a destination (x.x.x.x) that doesn't match control channel (y.y.y.y): possible Bounce attack? To enforce strict PORT checking please set "ftpd.allow_address_mismatch=False" in the Config.cf file."
```

If the firewall administrator decides that this is not a problem in their environment, they can disable this Warning message by setting the following Config.cf variable:

```
ftpd.suppress_address_mismatch_warning=True  
(default is False)
```

2) If the firewall administrator wishes to enforce strict PORT command checking and block any PORT requests that reference a different address than the original FTP client IP they can set the following Config.cf variable:

```
ftpd.allow_address_mismatch=False (default is True)
```

By enforcing "strict" PORT checking on the firewall, security administrators do not have to make sure that all of their FTP servers are patched or configured to block the FTP Bounce Attack.

These security enhancements were verified by Symantec and ICISA Labs. The new features will extend the enterprise-level protection provided by our FTP proxy which among other checks already includes protection against FTP Bounce attacks off the firewall itself, blocking PORT commands that select a well-known port, FTP strong/weak user authentication methods, GET/PUT granular security policies, FTP protocol and command verification, and transparent address hiding.

Technical Description:

The FTP Bounce attack exploits a known design flaw in the FTP standard. All RFC compliant FTP servers must support the PORT command. The PORT command is used between an FTP client and server to coordinate the data channel connection between the two devices. The RFC dictates that a connection for the data channel should be allowed to any IP address and any port. However, this RFC-compliance renders FTP Servers vulnerable to misuse of the PORT command. For a more detailed explanation of this issue,

Securiteam: [NEWS] Symantec Enterprise Firewall FTP Bounce Vulnerability (Patch Available)

please see CERT® Advisory CA-1997-27 FTP Bounce and the related technical tip.

The Symantec Enterprise Firewall automatically rewrites the PORT command with either the address of the client machine or the firewall address. In either case when the PORT request reaches the FTP server, the PORT command will match the source address of the FTP client. If configured, the FTP server scans the packet to make sure the PORT command matches the IP address of the client, and in all cases, it does. The FTP server then attempts to open a data connection to the client IP address, which then is translated by the firewall to the victim's IP address. This is not a desired behavior since it gives the security administrator a false sense of protection from an FTP bounce attack.

ADDITIONAL INFORMATION

The information has been provided by <mailto:waguilar@symantec.com>
William Aguilar.

=====

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: "[NT] Back Office Web Administration Authentication Bypass"
 - *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)