

[NT] Falcon Web Server Authentication Circumvention Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-02/0097.html>

From: support@securiteam.com

Date: 02/16/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 16 Feb 2002 17:43:00 +0100 (CET)

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.

Falcon Web Server Authentication Circumvention Vulnerability

SUMMARY

<<http://www.blueface.com/>> Falcon Web Server is an ISAPI and WinCGI supporting web server running on the Microsoft Windows OS's. A security vulnerability in the product allows bypassing of the server's security restrictions by requesting a specially formed URL request.

DETAILS

Vulnerable systems:

Falcon Web Server 2.0.0.1020 and prior

Immune systems:

Falcon Web Server 2.0.0.1021

Falcon Web Server supports virtual directory mapping and allows the server administrator to use a user-authentication scheme to protect the content of these directories. Due to a problem in the parsing of requests made to such directories it is possible to circumvent this authentication scheme and access any file in a protected directory without supplying the proper credentials.

Securiteam: [NT] Falcon Web Server Authentication Circumvention Vulnerability

The attack consists of adding an additional backslash at the beginning of the virtual path. For example, the server comes with one such path to a directory 'test' pre-configured, which requires authentication to be accessed. A direct request to this directory ("<http://server/test/>") without supplying the proper credentials will return a 401 Unauthorized error. Requesting the same directory as "<http://server//test/>" however, will allow the user access without authenticating.

Solution:

The vendor has been notified and has addressed this issue by releasing build 2.0.0.1021 for the Falcon Web Server Standard and SSL editions. This has been tested against Falcon Web Server builds 2.0.0.1009 and 2.0.0.1020 on Win2k.

ADDITIONAL INFORMATION

The information has been provided by
<<mailto:vuln-dev@labs.secureance.com>> Strumpf Noir Society.

=====

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: "[\[UNIX\] Add2it Mailman Command Execution \(File Writing\)](#)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)