

[NEWS] Netware Web Server Sample Page Source Disclosure

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-12/0083.html>

From: support@securiteam.com

Date: 12/20/01

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 20 Dec 2001 09:31:39 +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.

Netware Web Server Sample Page Source Disclosure

SUMMARY

Novell's Netware 5.1 ships with a Web Server that is installed by default and contains various sample web pages. There is a "viewcode" application that runs through a Netware Loadable Module (NLM), which allows the source code of a default web page to be viewed. However, the NLM has the sample page name passed to it through a URL containing the path to the file. It is possible to alter the URL to permit the contents of any file on the system to be viewed even those situated outside the web root. With this method, it is possible to view important configuration files including the autoexec.ncf file that contains the remote console password.

DETAILS

Vulnerable systems:

Netware Web Server version 5.1

Netware is an Operating System developed by Novell and used by many organizations for user file and print sharing. Version 5.1 of the Netware Operating system comes with a web server that is installed by default. Included on the web server are a wide variety of sample pages that demonstrate the flexibility and features of the product. However, one

Securiteam: [NEWS] Netware Web Server Sample Page Source Disclosure

sample page uses a Netware Loadable Module (NLM) called sewse.nlm to call a script called viewcode.jse. The viewcode.jse file displays the source code of sample files called httpplist.htm and httpplist.jse. These file names are passed as parameters to the NLM through a URL such as (URL may wrap):

[http://10.0.25.5/lcgi/sewse.nlm?](http://10.0.25.5/lcgi/sewse.nlm?sys:/novonyx/suitespot/docs/sewse/viewcode.jse+httpplist/httpplist.htm+httpplist/httpplist.jse)
sys:/novonyx/suitespot/docs/sewse/viewcode.jse+httpplist/httpplist.htm+httpplist/httpplist.jse

The application checks the files being requested by requiring that the httpplist directory is specified in the path to the files to be viewed. However, it is possible to traverse directories using ../ after httpplist. The sewse.nlm module runs with sufficient permissions whereby it possible to traverse to any files in the file system and view its content.

There are many files that may be of interest to an attacker and these include:

SYS:\ETC\NETINFO.CFG – Can contain a copy of the rconsole password
SYS:\SYSTEM\AUTOEXEC.NCF – Contains the rconsole password
SYS:\ETC\FTPAUDIT.LOG – Contains valid usernames for password guessing attempts

An attacker could use the information gained to launch further attacks or to gain console access using the rconsole password. An example of the URL used to view the autoexec.ncf is (URL may wrap):

[http://10.0.25.5/lcgi/sewse.nlm?](http://10.0.25.5/lcgi/sewse.nlm?sys:/novonyx/suitespot/docs/sewse/viewcode.jse+httpplist+httpplist/../../../../system/autoexec.ncf)
sys:/novonyx/suitespot/docs/sewse/viewcode.jse+httpplist+httpplist/../../../../system/autoexec.ncf

There are Novell best practices that include encrypting the rconsole password in the autoexec.ncf file. However, there are tools available that can be used to break this encryption. Another Novell recommendation is to use a Console Screensaver that requires the admin password to be entered after an rconsole connection has been made. This issue is similar to the problem discovered with the convert.bas script that shipped with Netware Web Server version 2.0.

Vendor & patch information:

The vendor of this product, Novell, was contacted via email using the address listed as their 'community relations' on 20 November 2001. When no reply was received to this email after nine days, another email was sent on 29 November 2001 to the same address, and copied to 'secure@novell.com'. No reply from either address had been received as of December 11 2001.

Workarounds:

A workaround involves removing all sample web pages and sample NLMs.

ADDITIONAL INFORMATION

Securiteam: [NEWS] Netware Web Server Sample Page Source Disclosure

The information has been provided by <mailto:advisories@irimplc.com> IRM Security Advisories.

=====

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] ProFTPD File Globbing Problems (////.../)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)