

[NT] Multiple Remote Buffer Overruns Tomahawk' SteelArrow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0063.html>

From: support@securiteam.com

Date: 08/20/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 20 Aug 2002 10:50:59 +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.

Multiple Remote Buffer Overruns Tomahawk' SteelArrow

SUMMARY

<<http://www.tomahawk.com/>> SteelArrow is an easy to use Web Application Server offering the latest in Internet connectivity and dynamic content development. SteelArrow offers developers full web application development functionality and fully tested run time reliability. SteelArrow operates as an extension (on WinNT/2K) to Microsoft IIS, Apache, and Netscape Enterprise servers. Multiple buffer overflows have been found in the product allowing a remote attacker to execute arbitrary code on the remote machine.

DETAILS

Buffer Overrun 1:

SteelArrow tracks user sessions with cookies in the form of UserID=XXXXXXXXXXXX. By supplying an overly long value in the Cookie HTTP header a buffer overflow occurs in the SteelArrow Service (Steelarrow.exe) overwriting a saved return address on the stack. SteelArrow, by default on Win2k/WinNT is installed as a system service. Any arbitrary code executed using this vulnerability will run with system privileges.

Securiteam: [NT] Multiple Remote Buffer Overruns Tomahawk' SteelArrow

Buffer Overrun 2:

By making an overly long request for an .ARO (extension used by SteelArrow) file, an access violation occurs in DLLHOST.EXE (Steelarrow.dll), again overwriting a saved return address on the stack. Any code will execute in the security context of the IWAM account.

Buffer Overrun 3:

This issue is very similar to the Chunked Transfer-Encoding issue. By making a request for an .ARO file including a specific Transfer-Encoding: Chunked request within the HTTP request header fields and access violation occurs in DLLHOST.EXE due to a heap overflow. Again, any arbitrary code execution will run in the context of the IWAM account.

Fix Information:

NGSSoftware alerted the vendor to these buffer overflow issues on the 1st 2nd and 3rd of April 2002. A fix is available from <http://www.steelarrow.com>.

ADDITIONAL INFORMATION

The information has been provided by <mailto:mark@ngssoftware.com> Mark Litchfield of NGSSoftware Insight Security Research.

=====

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] Bonsai XSS and Physical Path Revealing Vulnerabilities"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)