

[NT] Buffer Overrun in Talentsoft's Web+

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-03/0032.html>

From: support@securiteam.com

Date: 03/07/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 7 Mar 2002 17:39:33 +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.

Buffer Overrun in Talentsoft's Web+

SUMMARY

<<http://www.talentsoft.com>> Talentsoft's Web+ v5.0 is a powerful and comprehensive development environment for use in creating web-based client/server applications. Attackers can exploit a buffer overrun vulnerability in the product to execute arbitrary code as SYSTEM.

DETAILS

During installation webplus.exe is copied into the cgi-bin or scripts directory and is utilized by many of TalentSoft's products such as Web+ Shop, Web+ Mall and Web+ Enterprise. By supply an overly long character string to webplus.exe which is then passed to a system service -- webpsvc.exe. It is this service that overflows, overwriting the saved return address on the stack. Because Webpsvc by default is started as a system service, any arbitrary code executed on the server would run in the security context of the SYSTEM account.

Fix information:

NGSSoftware alerted TalentSoft to these problems on 12th February 2002.

Talentsoft has created a patch for this issue and NGSSoftware advises all

Web+ customers to apply this as soon as is possible.

Securiteam: [NT] Buffer Overrun in Talentsoft's Web+

Please see <<http://www.talentsoft.com/Issues/IssueDetail.wml?ID=WP943>>
<http://www.talentsoft.com/Issues/IssueDetail.wml?ID=WP943> for more
details.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:nisr@NEXTGENSS.COM>> David
Litchfield.

=====

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] OpenSSH Off-By-One Vulnerability"
 - *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)