

[NT] Microsoft SharePoint Portal and Team Services Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0090.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 11/23/03

To: list@securiteam.com

Date: 23 Nov 2003 11:13:52 +0200

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Microsoft SharePoint Portal and Team Services Vulnerability

SUMMARY

A vulnerability in the way Microsoft's SharePoint Portal and Team Services works, allows remote attackers to bypass the authentication mechanism, by disabling the JavaScript support when viewing that page (or restricting access to the password protected area). Disabling JavaScript doesn't not affect the ability to control the products.

DETAILS

There is a bug in how the authentication works with the web-based administration page. This page resides, in the web servers with SharePoint, in <http://www.example.com/layouts/settings.htm> or http://www.example.com/some_directory/layouts/settings.htm.

This page is usually protected by NT Basic or NTLM authentication via a JavaScript request to a protected area.

The trick to see this page consist in modifying the IE security sidebar, in Security tab, to HIGH, or by disabling JavaScript. The process is as follow:

Securiteam: [NT] Microsoft SharePoint Portal and Team Services Vulnerability

- Check Security: Tools -> Options -> Security -> Security Medium
- Browse to /_layouts/settings.htm page.
- NT Basic or NTLM Window is shown
- Click on Cancel -> You see "You are not authorized to view this page"
- Change Security to HIGH and press F5 for refresh
- The page is shown with some error and incomplete, but we don't need user or password to see it and some links are fully functional

ADDITIONAL INFORMATION

The information has been provided by <mailto:arkanian@hacker.am>
arkanian.

=====

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.