

[NT] Multiple XSS vulnerabilities in Microsoft SharePoint Portal Server

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-04/0020.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 04/07/04

To: list@securiteam.com

Date: 7 Apr 2004 16:48:10 +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>

Multiple XSS vulnerabilities in Microsoft SharePoint Portal Server

SUMMARY

"Microsoft

<<http://www.microsoft.com/PRODUCTS/info/product.aspx?view=22&pcid=69782349-8d48-4af5-94ed-3b00ae409>

SharePoint Portal Server provides an easy way to create Web portals with integrated document management services and search capabilities. You can establish a central point of access to all your existing key business information and applications, as well as share information across file servers, databases, public folders, Internet sites, and SharePoint Team Services-based Web sites."

Several cross-site scripting vulnerabilities have been found in SharePoint Portal.

DETAILS

Vulnerable Systems:

* Microsoft SharePoint Portal Server 2001 SP 2

Immune Systems:

* Microsoft SharePoint Portal Server 2001 SP 3

CVE Information:

Securiteam: [NT] Multiple XSS vulnerabilities in Microsoft SharePoint Portal Server

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0379>>
CAN-2004-0379

Three scripts of SharePoint Server have been found vulnerable to XSS attacks. They may lead to cookie/session stealing and running script code in the victim's browser context.

Patch Availability:

Microsoft has addressed the issue and made available for download SharePoint's Service Pack 3 that fixes the issues. It can be found at

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=15677A92-3470-465F-9F63-E621094103E0&display=details>>
<http://www.microsoft.com/downloads/details.aspx?FamilyId=15677A92-3470-465F-9F63-E621094103E0&display=details>

In addition, a description of the updates provided by SP3 can be found at

<<http://support.microsoft.com/default.aspx?kbid=http://support.microsoft.com?kbid=837017>>
<http://support.microsoft.com?kbid=837017>.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:ory.segal@sanctuminc.com>>
Ory Segal of Sanctum Inc..

=====

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.