

[NEWS] Portfolio Netpublish Server 'template' Directory Traversal

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00097.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 28 Dec 2005 12:08:19 +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>

Portfolio Netpublish Server 'template' Directory Traversal

SUMMARY

<http://www.extensis.com/en/products/asset_management/product_information.jsp?id=prod60022>
NetPublish Server from "Extensis is a database-driven file cataloging product, which is accessible via a web interface".

The NetPublish Server web interface is vulnerable to a directory traversal attack, which allows access to files that reside outside the web root directory.

DETAILS

Vulnerable Systems:
* Netpublish Server 7

Arbitrary files could be retrieved from the server by using a 'directory traversal' attack within the URL, as shown below:

<http://xxx.xxx.xxx.xxx/netpub/server.np?base site=XXXintra&catalog=catalog&template=../../../../../../../../boot.ini>

[NEWS] Portfolio Netpublish Server 'template' Directory Traversal

As a result of supplying the above URL the contents of the file 'boot.ini' are displayed in the web browser. Furthermore, by default the server runs with the privilege level of the local SYSTEM account (on Windows) and could therefore be used to retrieve the contents of any file on the server. The risk is reduced if the product is run on Unix, as the privilege level used is that of the 'nobody' account.

Vendor Status:

Extensis were contacted on October 11th 2005 and although they have not produced a patch to prevent the directory traversal they have released a KnowledgeBase article on their web site, which attempts to mitigate the issue. For more information see:

<http://www.extensis.com/en/support/kb_article.jsp?articleNumber=3302201>
http://www.extensis.com/en/support/kb_article.jsp?articleNumber=3302201

ADDITIONAL INFORMATION

The information has been provided by <<mailto:advisories@xxxxxxxxxx>>
[IRMPLC Advisories](#).

=====

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

=====

=====

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.

-
- Prev by Date: [\[UNIX\] PHPGedView Arbitrary Code Execution and Injection](#)
 - Next by Date: [\[UNIX\] Kpdf/Koffice Multiple Buffer Overflows \(Xpdf\)](#)
 - Previous by thread: [\[UNIX\] PHPGedView Arbitrary Code Execution and Injection](#)
 - Next by thread: [\[UNIX\] Kpdf/Koffice Multiple Buffer Overflows \(Xpdf\)](#)
 - Index(es):
 - ◆ [Date](#)
 - ◆ [Thread](#)