

[UNIX] ChurchInfo Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0022.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 08/07/05

To: list@securiteam.com

Date: 7 Aug 2005 17:19:42 +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>

ChurchInfo Multiple Vulnerabilities

SUMMARY

<<http://www.churchdb.org/>> ChurchInfo – "Free software to help churches track members, families, groups, pledges and payments."

ChurchInfo is affected by multiple path disclosures and SQL injections vulnerabilities.

DETAILS

Vulnerable Systems:

* ChurchInfo version 1.2.2 and prior

1) The "PersonID" parameter on the following pages are vulnerable to SQL injection and path disclosure:

PersonView.php

MemberRoleChange.php

PropertyAssign.php

WhyCameEditor.php

GroupPropsEditor.php

Reports/PDFLabel.php

UserDelete.php – First page gives path disclosure, then when you click yes you have sql injection

Securiteam: [UNIX] ChurchInfo Multiple Vulnerabilities

2) When an invalid "Number" parameter is provided to the following pages, a path disclosure vulnerability will occur:

SelectList.php

SelectDelete.php

3) The "DepositSlipID" parameter in the following page is vulnerable to SQL injection and path disclosure:

DepositSlipEditor.php

3) The "QueryID" parameter in the following page is vulnerable to SQL injection and path disclosure:

QueryView.php

In addition the following pages returned when you specify specific ids can be attacked with an SQL injection:

QueryID?id=18 The search box is vulnerable to SQL injection

QueryID?id=19 An sql injection can be performed by editing the HTML source of the form

4) The "GroupID" parameter in the following pages are vulnerable to SQL injection and path disclosure:

GroupView.php

GroupMemberList.php

MemberRoleChange.php

GroupDelete.php

/Reports/ClassAttendance.php

/Reports/GroupReport.php

5) The "GroupID" parameter in the following pages returns a path disclosure response when an invalid input is given to them:

GroupPropsFormRowOps.php

/Reports/ClassAttendance.php

/Reports/ClassList.php

ConfirmLabels.php

/DirectoryReport.php

/Reports/NewsLetterLabels.php

6) The "PropertyID" parameter in the following page is vulnerable to SQL injection and path disclosure:

PropertyEditor.php

7) The "FamilyID" parameter in the following pages are vulnerable to SQL injection and path disclosure:

Canvas05Editor.php

CanvasEditor.php

FamilyView.php

8) The "PledgeID" parameter in the following page is vulnerable to SQL injection and path disclosure:

PledgeDetails.php

Securiteam: [UNIX] ChurchInfo Multiple Vulnerabilities

ADDITIONAL INFORMATION

The information has been provided by <mailto:thegreatone2176@yahoo.com>
thegreatone2176.

=====

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.