

[UNIX] Multiple Vulnerabilities in Kayako eSupport

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0055.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/20/04

To: list@securiteam.com

Date: 20 Dec 2004 18:06:04 +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>

Multiple Vulnerabilities in Kayako eSupport

SUMMARY

<<http://www.kayako.com/>> Kayako eSupport is "one of the most feature packed support systems; in this tour you will find why over a thousand companies have decided to opt for eSupport and use it to process their daily support requests".

The Kayako eSupport product has been found to contain multiple vulnerabilities that range from cross site scripting issues to SQL injection vulnerabilities.

DETAILS

Cross Site Scripting:

A cross site scripting vulnerability exists in Kayako eSupport. This vulnerability exists due to user supplied input not being checked properly. Below is an example.

[http://path/index.php? a=knowledgebase& j=search&searchm=\[CODEGOESHERE\]](http://path/index.php? a=knowledgebase& j=search&searchm=[CODEGOESHERE])

This vulnerability could be used to steal cookie based authentication credentials within the scope of the current domain, or render hostile code in a victim's browser.

Securiteam: [UNIX] Multiple Vulnerabilities in Kayako eSupport

SQL Injection:

Kayako eSupport is prone to SQL Injection in a number of places. Below are some examples of URL's that could be used to take advantage of these vulnerabilities.

- [http://path/index.php? a=knowledgebase& j=subcat& i=\[SQL\]](http://path/index.php? a=knowledgebase& j=subcat& i=[SQL])
- [http://path/index.php? a=knowledgebase& j=rate& i=\[SQL\]&type=no](http://path/index.php? a=knowledgebase& j=rate& i=[SQL]&type=no)
- [http://path/index.php? a=knowledgebase& j=questiondetails& i=\[SQL\]](http://path/index.php? a=knowledgebase& j=questiondetails& i=[SQL])
- [http://path/index.php? a=tickets& m=viewmain&email22=blah@blah&ticketkey22=\[SQL\]](http://path/index.php? a=tickets& m=viewmain&email22=blah@blah&ticketkey22=[SQL])
- [http://path/index.php? a=tickets& m=viewmain&email22=\[SQL\]&ticketkey22=](http://path/index.php? a=tickets& m=viewmain&email22=[SQL]&ticketkey22=)

These is also an SQL Injection vulnerability in the "Home > Ticket Status > *Forgot Key*" feature. This can be take advantage of by putting a malicious query in the email field. Because of the location of the unchecked variable in the query, it makes it easy for an attacker to use these issues to query just about any info from the underlying database. It should also be noted that the attacker does not need to be logged in to Kayaki eSupport in order to exploit these SQL injections.

ADDITIONAL INFORMATION

The information has been provided by <mailto:security@gulftech.org> GulfTech Security.

The original article can be found at:

- <http://www.gulftech.org/?node=research&article_id=00056-12182004>
- http://www.gulftech.org/?node=research&article_id=00056-12182004

=====

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.