

[UNIX] Information Disclosure and SQL Injection in iGeneric eShop

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0100.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 02/24/05

To: list@securiteam.com

Date: 24 Feb 2005 17:32:58 +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>

Information Disclosure and SQL Injection in iGeneric eShop

SUMMARY

"Create a robust full featured online shop within minutes with http://www.igeneric.co.uk/display_resources/resource1.html> iG Shop. iG Shop is a powerful PHP MySQL based shopping cart system that enables you create full featured online shop very quickly."

Multiple SQL Injection vulnerabilities were discovered in iGeneric eShop software, allowing a remote attacker to modify the product's existing SQL statements with his own arbitrary SQL statements.

DETAILS

Vulnerable Systems:

* iGeneric eShop version 1.2

Proof of Concept:

[http://www.victimsite.com/page.php?page_type=catalog_products&type_id\[\]=2&SESSION_ID=304ba47f3ea48f0d6e1acdd6480c2c9c&page_type=catalog_products&cats='](http://www.victimsite.com/page.php?page_type=catalog_products&type_id[]=2&SESSION_ID=304ba47f3ea48f0d6e1acdd6480c2c9c&page_type=catalog_products&cats=')

[http://www.victimsite.com/page.php?page_type=catalog_products&type_id\[\]=2&](http://www.victimsite.com/page.php?page_type=catalog_products&type_id[]=2&)

Securiteam: [UNIX] Information Disclosure and SQL Injection in iGeneric eShop

SESSION_ID=304ba47f3ea48f0d6e1acdd6480c2c9c&page_type3=catalog_products&search=1&l_price='&u_price=1&Submit=Search

[http://www.victimsite.com/page.php?page_type=catalog_products&type_id\[\]=2&SESSION_ID=304ba47f3ea48f0d6e1acdd6480c2c9c&page_type3=catalog_products&search=1&l_price=1&u_price='&Submit=Search](http://www.victimsite.com/page.php?page_type=catalog_products&type_id[]=2&SESSION_ID=304ba47f3ea48f0d6e1acdd6480c2c9c&page_type3=catalog_products&search=1&l_price=1&u_price='&Submit=Search)

Disclosure Timeline:

- * 10/02/2005 – Vulnerabilities found
- * 14/02/2005 – Vendor informed.
- * 20/02/2005 – Public notice.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:johnc@nobytes.com>> John Cobb.

The original article can be found at: <<http://www.nobytes.com>>
<http://www.nobytes.com>

=====

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.