

[UNIX] Aardvark Topsites Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0059.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/18/03

To: list@securiteam.com

Date: 18 Dec 2003 16:25:05 +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>

Aardvark Topsites Multiple Vulnerabilities

SUMMARY

<<http://www.aardvarkind.com>> Aardvark Topsites is "a popular free PHP Topsites script". Multiple vulnerabilities have been found in the product allowing remote attacker to disclosure sensitive information about the server and inject malicious SQL statements.

DETAILS

Vulnerable systems:

- * Aardvark Topsites PHP version 4.1.0 and prior

Immune systems:

- * Aardvark Topsites PHP version 4.1.1

Plaintext Database Password Weakness:

The login info for the database being used by Aardvark Topsites can be viewed in plaintext by anyone who has access to the admin panel. If an attacker can gain access to the admin panel, he can then take control of the database that the Aardvark Topsites is using.

Information Disclosure Vulnerability:

By default `phpinfo()` for the server hosting an Aardvark Topsite can be

Securiteam: [UNIX] Aardvark Topsites Multiple Vulnerabilities

viewed in the sources directory [/sources/info.php] An easy work around for this is quite obvious. If you do not need this file delete it.

Path Disclosure Vulnerability:

There are multiple ways to disclose the full server path on an Aardvark Topsites. Most can be avoided by allowing visitors to the /sources/ directory. However, it is also possible by passing a null or invalid value to the "type" variable when viewing the graph feature.

Example:

<http://vulnerablesite/index.php?a=graph&id=1&type=>

SQL Injection Vulnerability:

Tampering with SQL queries is possible via the "method" variable in display.php. You can test if you are vulnerable by accessing the URL below.

Example:

<http://vulnerablesite/index.php?method=>'

In addition, these are prone to tampering. While it would be hard to exploit, the following should have input validated/sanitized a little better.

<http://vulnerablesite/index.php?a=lostopw&set=1&id=>'

http://vulnerablesite/index.php?a=lostopw&set=1&session_id='

Solution:

Aardvark Industries were very prompt and professional in addressing these issues. You can now download Aardvark Topsites 4.1.1 that has new features along with the obvious security fixes. The latest version is available from <<http://www.aardvarkind.com/index.php?page=downloads>>
<http://www.aardvarkind.com/index.php?page=downloads>.

ADDITIONAL INFORMATION

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

=====

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,

Securiteam: [UNIX] Aardvark Topsites Multiple Vulnerabilities

loss of business profits or special damages.