

[VulnWatch] Happymall E-Commerce Remote Command Execution

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-05/0009.html>

From: SecurityTracker (help_at_securitytracker.com)

Date: 05/08/03

Date: Wed, 07 May 2003 18:03:21 -0400

To: vulnwatch@vulnwatch.org

Advisory URL: <http://securitytracker.com/alerts/2003/May/1006707.html>

Vendor: Happycgi.com

Product: Happymall

Versions: 4.3, 4.4

Title: Happymall E-Commerce Input Validation Flaw Lets Remote Users Execute Arbitrary Commands

Description: Revin Aldi reported an input validation vulnerability in the Happymall e-commerce software. Two scripts allow remote users to execute arbitrary commands with the privileges of the web server.

The 'normal_html.cgi' script does not filter user-supplied input before making an open() call based on that input. A remote user can create a specially crafted URL to cause the system to execute arbitrary operating system commands.

A demonstration exploit is provided:

```
/shop/normal_html.cgi?file=|id|
```

```
/shop/normal_html.cgi? file=;id|
```

The vendor reports that the 'member_html.cgi' script is also affected.

Impact: A remote user can execute arbitrary shell commands with the privileges of the target web server.

Solution: The vendor has issued a fix. See the attached CERT-KR advisory for more information.

Credit: revin aldi (reVn@minangCrew.Web.Ma) discovered and reported this flaw to SecurityTracker and sends Greetz to #MinangCrew at Dal.Net

VulnWatch: [VulnWatch] Happymall E-Commerce Remote Command Execution

CVE: CAN-2003-0243

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0243>

Timeline:

Apr 26, 2003 Reported to SecurityTracker
Apr 27, 2003 Vendor contacted (via English language e-mail, without response)
Apr 29, 2003 CERTCC-KR initially contacted
May 2, 2003 Details of vulnerability provided to vendor
May 3, 2003 CERTCC-KR Advisory published

Distribution: The above SecurityTracker text is Copyright 2003 by SecurityGlobal.net LLC but can be redistributed without restrictions.

Additional Information: The CERTCC-KR advisory is shown below.

=====
KA-2003-33: The Vulnerability of File Open Function in Happymall,
an application of e-commerce.

Published : May 03, 2003
Updated : May 03, 2003
Reference : <http://www.certcc.or.kr>

-- Systems Affected -----
All web servers running Happymall version 4.3 and 4.4 only

-- Impact -----
The normal_html.cgi and member_html.cgi script of Happymall allow a remote user to execute arbitrary operating system commands on the web server with the privilege of web server.

-- Description -----
Happymall is an application being used in some e-commerce sites. Following is what the problem is.

1. If you open normal_html.cgi or member_html.cgi you can find that there is a sentence, open (A, "\$admin_path/normal_html/\$END{'file'}") or die print "\$END{'file'}", which happens to perl programming from time to time.
2. \$END{'file'} is looking for file itself in the server to get the value of file.
3. A Remote user possibly exploits a system running Happymall using this vulnerability only when the value of file is system function.

-- Solution -----
Apply Patch downloaded from :
http://happymall.happycgi.com/forum/forum_detail.cgi?thread=353

How to apply patch to the system :

VulnWatch: [VulnWatch] Happymall E-Commerce Remote Command Execution

1. Extract zip file downloaded and you will get two files, member_html.cgi and normal_html.cgi.
2. Upload those files with ASCII mode to the web server in the directory containing index.cgi and overwrite.

3. Change the linked address

For example;

Before patch applied : http://test6.happycgi.com/normal_html.cgi?file=company.html

After patch applied : http://test6.happycgi.com/normal_html.cgi?file=company

--- Reference Sites -----

<http://www.certcc.or.kr>

<http://happymall.happycgi.com>

Korea Information Security Agency, KISA

Computer Emergency Response Team Coordination Center, CERTCC-KR

Hot Line: 02-118 Email: cert@certcc.or.kr
=====