

[UNIX] GuppY Directory Traversal and Database Corruption

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00046.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 16 Mar 2006 13:59:16 +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>

GuppY Directory Traversal and Database Corruption

SUMMARY

<<http://www.freeguppy.org>> GuppY is a web portal intentionally designed to be easy to use for you, the final user. It doesn't require any database to run.

A remote attacker can overrun the application database with arbitrary content and perform a directory traversal attack.

DETAILS

Vulnerable Systems:

- * GuppY version 4.5.11 and lower

Immune Systems:

- * GuppY version 4.5.12

When GuppY is installed with `magic_quotes_gpc = Off`, a remote attacker can write arbitrary content to the database via NULL injection in the `gp` parameter in `dwild.php`. Furthermore, the filter of the parameter can be bypassed by using `%2E/` instead of `../` thus allowing directory traversal.

[UNIX] GuppY Directory Traversal and Database Corruption

Vulnerable Code:

```
//dwnld.php
$dndcounter = ReadDocCounter(DBBASE.$pg);
UpdateDocCounter($pg);

//log.inc
}
WriteDBFields(DBLOGH,$dblog);
}
$stabcounter = CompteVisites(DBIPSTATS, DBSTATS);
if ($stabcounter[0] > 0 && ($stabcounter[0]/10) ==
intval($stabcounter[0]/10)) {
WriteCounter(DBSTATSBK, $stabcounter[0]);
}

//functions.php
function WriteCounter($fic,$DataDB) {
$fhandle = fopen($fic, "w");
fputs($fhandle, $DataDB."\n");
fclose($fhandle);
}
```

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

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.